

CompTIA Network+ Exam Notes

LAN Technologies

1. LAN Media Access

LAN Media Access Basics

- 1.1 **Media access technologies** deal with how devices communicate with each other over a physical transmission medium.
- 1.2 The **collision problem** exists if a **shared** physical transmission medium is used for data transmission. If more than one device tries to send frames at the same time, the frames will corrupt each other in the shared medium.
- 1.3 The devices that share the same physical transmission medium are in the same **collision domain**. A frame sent by a device can cause collision with a frame sent by another device in the same collision domain. Moreover, a device can hear the packets destined to any device in the same domain, i.e. sniffing.
- 1.4 **Contention technology** refers to any media access technology that requires devices to share the same physical transmission medium and compete for the same resource, e.g. CSMA/CD.
- 1.5 Repeaters do not break up collision domains, whereas bridges, switches or routers do. (Details about repeaters, bridges, switches and routers can be found in Section 4).
- 1.6 A **Media Access Control (MAC) address** (also known as physical address or hardware address) is the data link layer address of a computer. It is programmed into the ROM of the computer's network interface card (NIC). MAC addresses are used by a bridge or switch to forward frames in the same network segment (IP addresses are used by a router to route packets across network segments).
- 1.7 There are 3 types of MAC address. They are:
 - **Unicast** address - an address for a specific computer.
 - **Multicast** address - an address for a specific group of computers.

- **Broadcast** address - an address for all the computers in a network.

1.8 **Address Resolution Protocol (ARP)** maps IP addresses to the associated MAC addresses for the devices in the same network segment (i.e. locally attached devices). For example, Computer A wants to send a packet to Computer B. Based on B's IP address, it is known that B is on the same network segment as A (details about IP routing can be found in Chapter 4). Therefore, A needs to find out the MAC address of B to pass the frame to B. It happens as follows:

1. A checks its ARP cache for the mapping of B's IP address to the MAC address.
2. If there is no entry in the ARP cache for B, A broadcasts (Layer 2 broadcast) an ARP request for the IP address of B.
3. B replies to the ARP request (with its MAC address).
4. A sends the frame to the MAC address replied by B and stores the IP-address-to-MAC-address mapping into its ARP cache.

1.9 **Reverse Address Resolution Protocol (RARP)** maps a MAC address to the associated IP address. It is usually used by a diskless client to obtain an IP address during a system boot-up. It works as follows:

- When a client boots up, it broadcasts (Layer 2 broadcast) a RARP request with its MAC address.
- A RARP server looks up its table for the entry corresponding to this MAC address.
- If the entry is found, the server responds with the associated IP address.
- The client uses this IP address as its own address.

1.10 **Boot Protocol (BOOTP)** and **Dynamic Host Configuration Protocol (DHCP)** both provide similar functions as RARP but with enhanced features, e.g. providing the name server address and the default gateway address to the client. DHCP is the most popular one among the three protocols. Details about DHCP can be found in Chapter 5.

LAN Media Access Methods

1.11 There are several major types of **LAN media access methods**. They are:

- **Carrier Sense Multiple Access / Collision Detection (CSMA/CD)**.
- **Carrier Sense Multiple Access / Collision Avoidance (CSMA/CA)**.
- **Token passing**.
- **Polling**.

1.12 In a **CSMA/CD** network, all the computers monitor the **carrier activities** (i.e. frame transmissions) on the shared medium continuously. If a computer wants to send a

frame, it needs to go through the following process:

1. The source computer will begin transmission when there is no carrier activity on the medium. All computers continue to listen for any collision.
2. If there is a collision (voltage increases above a threshold because of overlapping signals), the source computer will abort the transmission. Every computer in the collision domain will execute the **back-off algorithm**, i.e. will not attempt to transmit any frame until its random collision timer expires.
3. The source computer attempts to retransmit the frame by going through the whole cycle again after its collision timer expires.

1.13 In a **CSMA/CD** network, the following factors will increase the **collision rate**:

- Too many computers in a collision domain.
- Too many repeaters.
- Cable or connector defect.
- Cable length exceeds the recommended length limit.

1.14 In a **CSMA/CA** network, a computer shows its intention to transmit frames, by sending a "Request to send" (RTS) packet and waiting for a "Clear to send" (CTS) packet, before the actual transmission. The other computers in the same collision domain will then not attempt to transmit frames. Therefore there is **no collision** in a CSMA/CA network.

1.15 In a **token passing** network, a **token** (a control frame) is used to control which computer can put frames onto the medium. If a computer wants to send a frame, it needs to go through the following process:

1. The source computer waits for the token.
2. When the source computer receives the token, it appends its message to the token and passes the resulted frame to the next computer.
3. Each computer checks if the message is destined for itself. If so, it makes a copy of the message and marks the frame as read. If not, it just passes the frame to the next computer.
4. When the read frame is passed back to the source computer, the source computer removes the message from the frame and passes the remaining token to the next computer.

1.16 **CSMA/CD** networks and **token-passing** networks have the following differences:

- **CSMA/CD** networks are **non-deterministic**, while **token-passing** networks are **deterministic**, i.e. it is possible to calculate the maximum time that will pass before a station can transmit a frame successfully.
- The performance of a **token-passing** network **degrades gracefully** as the network

traffic increases. However, the performance of a **CSMA/CD** network **degrades sharply** when the network traffic exceeds a certain threshold because of excessive collisions.

1.17 In a **polling** network, the primary station asks the secondary stations periodically if they have anything to transmit. A secondary station cannot initiate a transmission by itself. Polling is commonly used in the mainframe environment.

2. LAN Protocols

2.1 **Ethernet** is the most common LAN protocol. Details about Ethernet can be found in the next section.

2.2 **Token Bus (IEEE 802.4)** is physically a linear **bus** or tree-shaped cable to which computers are attached. Logically, the computers are organized into a **ring** and a **token** is passed around the ring. A computer can send a frame only if it is holding the token.

2.3 **Token Ring (IEEE 802.5)** was developed by IBM. It has the following characteristics:

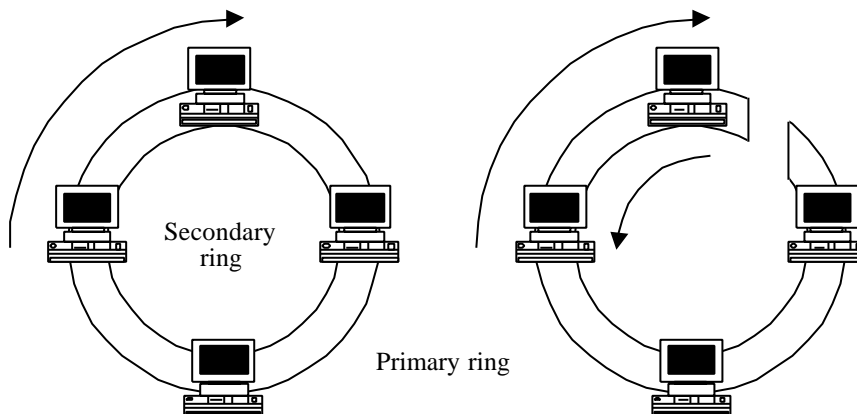
- It has a physical **star** topology. The central hub is called the **Multi-Station Access Unit (MAU or MSAU)**. All the computers are connected to it through twisted-pair cabling.
- It has a logical **ring** topology (at Layer 2).
- It uses the **token passing** technology. A token is passed around the ring.
- It runs either at **4 Mbps** or **16 Mbps**.
- The maximum number of stations per ring is **260** if STP is used, and **72** if UTP is used.
- There can be up to **33 MAUs** per ring. Each MAU has a *Ring Out* port and a *Ring In* port. The *Ring Out* port of the first MAU should be connected to the *Ring In* port of the second MAU, the *Ring Out* port of the second MAU should be connected to the *Ring In* port of the third MAU, and so on. The *Ring Out* port of the last MAU should be connected to the *Ring In* port of the first MAU to complete the ring.
- The maximum distance between a station and the MAU is **100m** if STP is used, and **45m** if UTP is used.
- It uses special hermaphroditic connectors for STP, known as **IBM Type-1 connector** or IBM-type Data Connector / Universal Data Connector (IDC/UDC).
- It has **self-recovering** mechanisms for exception handling:
 - A computer in the ring is designated as the **Active Monitor**, which is responsible to clean up garbled or orphan frames, detect for lost token and re-generate a new

token if necessary.

- If a computer notices that there is a problem in the network, it will send a **beacon frame** downstream to detect how many computers are down and then delete them from the ring. This mechanism is known as **beaconing**.
- Though token ring is designed to be fault tolerant, if a computer is working at a transmission speed different from the other computers, or if two computers in a ring have the same MAC address, the whole ring can be affected.

2.4 **Fiber Distributed Data Interface** or **FDDI (IEEE 802.8)** has the following characteristics:

- It uses the **token passing** technology and works like a **token ring**.
- It uses **fiber optics** cabling.
- It runs at **100 Mbps** and covers up to **100 km**. It is mainly used as the backbone of a network.
- It supports **multiple tokens** in a fiber optics ring for simultaneous communications.
- It supports fault tolerance by using **dual rings**.
- The primary ring passes frames in a clockwise direction. The secondary ring is a standby ring and passes frames in an anti-clockwise direction when it is in use (i.e. when the primary ring has problem). A sensor watches the primary ring continuously. If a problem is found, the sensor will invoke a ring wrap to isolate the failed part of the ring.



Primary ring functioning normally.

Part of the primary ring failed.

A ring wrap is triggered to isolate the failed part.

- A station on an FDDI network can be a dual-attached station (DAS, i.e. attached to both rings), or a single-attached station (SAS, i.e. attached to only one ring).
- **Copper Distributed Data Interface (CDDI)** refers to FDDI over UTP, which can be used in a LAN environment in place of FDDI.

2.5 **100-VG-AnyLAN (IEEE 802.12)**, also known as **100Base-VG**, is a **100 Mbps** LAN technology. It was first developed by HP. It uses the **demand priority access method** (DPAM) and is incompatible with Ethernet. This technology is not commonly used.

3. Ethernet Technologies

3.1 **Ethernet** is the most common LAN technology. It consists of a family of protocols and standards in the **physical layer** and the **data link layer**. There are several versions of Ethernet as follows:

- **Ethernet I** - The original Ethernet, which was developed by Xerox.
- **Ethernet II** (also known as **DIX Ethernet**) - The second version of Ethernet, which was developed by DEC, Intel and Xerox.
- **IEEE 802.3** - IEEE Ethernet standard. It was released in 1980.

3.2 Ethernet has the following characteristics:

- It uses shared medium (coaxial cables, or twisted pair cables with hubs) to connect network devices.
- It uses CSMA/CD technology.
- Its performance begins to degrade because of collision problem if its utilization rate exceeds 30%.
- It has a physical bus (if coax is used) or star (if twisted pair cables and a hub/switch are used) topology.
- It has a logical bus topology (i.e. whenever a host transmits, the signal must run from one end of the network segment to the other end) if coax, or twisted pair cables and a hub, are used to connect the devices. However, if twisted pair cables and a switch are used to connect the devices, it has a logical star topology (because a switch breaks collision domains).
- It runs at 10 Mbps.
- It supports half-duplex or full-duplex.
- It allows the maximum frame size of 1,518 bytes (including 18 bytes for frame header and trailer), i.e. MTU of 1,500 bytes.
- It allows the minimum frame size of 64 bytes (including 18 bytes for frame header and trailer). If the data to be transmitted is less than 46 bytes, pad bytes are inserted to ensure that the frame is long enough.
- The IEEE 802 standard uses 802.3 for MAC sub-layer and 802.2 for LLC sub-layer.

3.3 There are three types of **Ethernet framing** (i.e. definition of fields in an Ethernet frame):

Ethernet II (DIX)

Preamble (8 bytes)	Dest. addr. (6 bytes)	Source addr. (6 bytes)	Type (2 bytes)	Data (46-1500 bytes)	FCS (4 bytes)
-----------------------	--------------------------	---------------------------	-------------------	-------------------------	------------------

IEEE 802.2 (SAP)

Preamble (8 bytes)	Dest. addr. (6 bytes)	Source addr. (6 bytes)	Length (2 bytes)	DSAP (1 byte)	SSAP (1 byte)	Control (1 byte)	Data (43-1497 bytes)	FCS (4 bytes)
-----------------------	--------------------------	---------------------------	---------------------	------------------	------------------	---------------------	-------------------------	------------------

← 802.3 MAC → ← 802.2 LLC →

IEEE 802.2 (SNAP)

Preamble (8 bytes)	Dest. addr. (6 bytes)	Source addr. (6 bytes)	Length (2 bytes)	DSAP (1 byte)	SSAP (1 byte)	Control (1 byte)	SNAP (5 bytes)	Data (38-1492 bytes)	FCS (4 bytes)
-----------------------	--------------------------	---------------------------	---------------------	------------------	------------------	---------------------	-------------------	-------------------------	------------------

← 802.3 MAC → ← 802.2 LLC → 802.2 SNAP

- The MAC headers and trailers of the three framing types are identical for compatibility.
- The **Preamble** contains 7 bytes of alternating 1,0 bit pattern, and ends with a 1-byte **Start-of-frame delimiter** (SFD) of pattern 10101011. The receiving device uses the preamble to detect the beginning of the Ethernet frame. The preamble is not included as part of the frame when calculating the maximum frame size of 1,518 bytes.
- Ethernet **MAC address** has the following characteristics:
 - It is **6 bytes** long.
 - Each Ethernet MAC address is **unique**.
 - It is usually written as three sets of four hex digits that are separated with periods, e.g. 09D7.1A3B.249A.
 - It is burnt into the ROM of the NIC and cannot be changed. It is also known as hardware address, burned-in address (BIA), or universally administered address (UAA). However, many operating systems (e.g. Windows XP and Linux) allow a locally administered address (LAA) to override the factory MAC address.
 - The first half (24 bits) of the address identifies the NIC manufacturer, and is known as the Organizationally Unique Identifier (OUI), which is assigned by IEEE to the manufacturer.
 - The second half (24 bits) of the address is assigned by the NIC manufacturer, and is sometimes referred to as the Device ID.
 - Ethernet **broadcast address** has a value of FFFF.FFFF.FFFF.
 - Ethernet **multicast addresses** are in the range of 0100.5E00.0000 - 0100.5EFF.FFFF.
 - The source and destination MAC addresses are transmitted with the least significant bit (LSB) first.
- The **Frame Check Sequence** (FCS) or **Cyclic Redundancy Check** (CRC) field

contains a checksum for detecting errors in the rest of the frame.

- The Ethernet II **Type** field is used to specify the type of data that follows the Ethernet header (e.g. 0800 for IP, 8137 for Netware).
- The 802.3 **Length** field specifies how many bytes follow, excluding the FCS. Since none of the valid 802.3 **Length** values is the same as the valid Ethernet II **Type** values, 802 and Ethernet II frame formats are distinguishable.
- The 802.2 **Destination Service Access Point (DSAP)** and **Source Service Access Point (SSAP)** fields are used to specify the type of data that follows if the SNAP header is not used (e.g. E0 for Netware, 04 for SNA). If the SNAP header is used, both the DSAP and the SSAP always have the value of "0xAA" (0x stands for hexadecimal value), and the Control field has the value of "0x03".
- The 802.2 **Sub-network Access Protocol (SNAP)** field contains a 3-byte OUI field (typically be zero) and a 2-byte Type field (equivalent to the Ethernet II Type field).

3.4 **Fast Ethernet (IEEE 802.3u)** uses similar technologies as Ethernet (e.g. CSMA/CD, Ethernet frame format) and is compatible with Ethernet, but runs at **100 Mbps**.

3.5 **Gigabit Ethernet (IEEE 802.3z for optical cabling and 802.3ab for electrical cabling)** runs at **1 Gbps**.

3.6 **10 Gigabit Ethernet (IEEE 802.3ae)** runs at **10 Gbps**. It has some differences with the other types of Ethernet protocols:

- It only allows point-to-point topology.
- It only allows full-duplex communication.
- It only runs on fiber optics cables.

3.7 There are different implementations of Ethernet, Fast Ethernet and Gigabit Ethernet using different cabling standards:

Implementation	Cable type	Transmission rate	Distance limit
10Base2	Thinnet	10 Mbps	185 m
10Base5	Thicknet	10 Mbps	500 m
10Base-T	UTP Cat 3 or above, 2 wire-pairs are used	10 Mbps	100 m
10Base-FL	Fiber optics	10 Mbps	Multi-mode - 2 km Single-mode - 10 km
100Base-T4	UTP Cat 3 or above, 4 wire-pairs are used	100 Mbps	100 m
100Base-TX	UTP Cat 5 or above, 2 wire-pairs are used	100 Mbps	100 m
100Base-FX	Fiber optics	100 Mbps	Multi-mode - 2 km Single-mode - 10 km

1000Base-SX	Fiber optics - short wavelength	1 Gbps	Multi-mode - 550m
1000Base-LX	Fiber optics - long wavelength	1 Gbps	Multi-mode - 550m Single-mode - 10 km
1000Base-ZX	Fiber optics - extended wavelength	1 Gbps	Single-mode - 100 km
1000Base-CX	STP, 2 wire-pairs are used	1 Gbps	25 m
1000Base-T	UTP Cat 5 or above, 4-pair	1 Gbps	100 m
10GBase-SR	Fiber optics - short wavelength	10 Gbps	Multi-mode - 300m
10GBase-LR	Fiber optics - long wavelength	10 Gbps	Single-mode - 10 km
10GBase-ER	Fiber optics - extra long wavelength	10 Gbps	Single-mode - 40 km

3.8 **Half-duplex** Ethernet uses only **one pair** of wires for data transmission, while **full-duplex** Ethernet uses **two pairs** of wires. A typical half-duplex Ethernet network is only about 30 - 40% efficient at most. A full-duplex Ethernet network can be 100% efficient in both directions (e.g. 10Mbps per direction in a 10BaseT network) in theory because there is no collision.

3.9 A **DIX Ethernet** network uses **10Base2** or **10Base5** (**10** refers to 10Mbps, **Base** refers to baseband technology is used, **2** and **5** refers to the distance limit of approximately 200m and 500m respectively) for cabling. It has the following characteristics:

- There is no hub or switch.
- It has a **bus topology** both physically and logically.
- A series of cables forms an electrical bus that is shared by all the devices on the network.
- The devices must operate in **half-duplex** mode because if a device is sending and receiving frames at the same time (which is allowed under full-duplex mode), a collision occurs.
- Failure of any one device will affect the whole network.

3.10 A **10Base-T** or **100Base-T** network using **hubs** has the following characteristics:

- All devices are connected to a **central hub** (or through other hubs to the central hub).
- Physically, it is a **star topology**.
- Logically, all the devices share a single 10 Mbps or 100 Mbps **bus**.
- The devices must operate in **half-duplex** mode because if a device is sending and receiving frames at the same time, a collision occurs.

- Failure of a device does not affect the other devices. However, there is a single point of failure at the central hub.

3.11 A **10Base-T** or **100Base-T** network using **switches** has the following characteristics:

- All devices are connected to a **central switch** (or through other switches to the central switch).
- A switch creates a single bus for each port. Therefore, the network has a **star** topology both physically and logically.
- If only one device is connected to each port, there is **no collision** and the device can operate in **full-duplex** mode. The CSMA/CD logic can be disabled.
- Each port of a switch has its own bandwidth, i.e. 10 Mbps or 100 Mbps per port.

3.12 A **10/100 card** is a NIC that can support both Ethernet and Fast Ethernet. It can **auto-negotiate** with the connected device (e.g. a switch) to run at 10 Mbps or 100 Mbps, half-duplex or full-duplex (default = half-duplex 10 Mbps). **10/100/1000 cards** are also available in the market.

3.13 However, the auto-negotiation process may sometimes fail (e.g. the switch port runs at half-duplex but the computer runs at full-duplex incorrectly after the auto-negotiation, causing a lot of collisions). Therefore, it is recommended to disable the auto-negotiation feature and statically configure the parameters on a server and the switch port that is connected to the server. The feature should be enabled only for end-user devices, which may be moved frequently.

4. LAN Devices

4.1 A **network interface card** (NIC) has the following characteristics:

- It works at the physical and data-link layer.
- It is either an expansion card installed in a computer, or is built-in to the motherboard of a computer, to connect the computer to the network.

4.2 A **repeater** is a LAN device with the following characteristics:

- It works at the physical layer.
- It regenerates and amplifies digital signals from one cable segment to another.
- It extends a network over a greater distance.
- All the connected devices are in the same collision domain.
- The **5-4-3 Rule** states that no two hosts in an Ethernet collision domain may be separated by more than 5 segments, which are connected by 4 repeaters, with 3 of the

segments populated (i.e. 2 of the segments have no connected host, and are simply used for extending the distance of the network). For example, the maximum distance of a 10Base5 network can be extended to 2500m (500m x 5 segments) with repeaters.

4.3 A **hub** has the following characteristics:

- It is a multi-port repeater.
- It connects multiple LAN devices together and forwards the signals received from one port to all the other active ports. Therefore, it is a **physical star**, but **logical bus** topology.
- There are two types of hubs:
 - **Passive hub** - It does not regenerate data signals like regular hubs (i.e. active hubs), but simply passes the signals along. The maximum segment distance allowed is shortened. It is rarely used nowadays.
 - **Active hub** - It regenerates data signals when forwarding them.

4.4 A **Multi-Station Access Unit** (MAU or MSAU) has the following characteristics:

- It is the hub in a token ring network. All hosts in the ring are connected to it.
- It regenerates and forwards data signals it received. However, the signals are only forwarded to the next active downstream port, instead of all ports. Therefore, it creates a logical ring data path.

4.5 A **bridge** has the following characteristics:

- It works at the data link layer.
- It connects multiple LAN segments together and extends a network over a greater distance.
- It is also known as a **transparent bridge** because the connected devices do not aware of the existence of the bridge.
- It forwards a frame based on the destination MAC address of the frame.
- It maintains a **forwarding table** (also known as **bridge table**). Each entry in the table maps a **destination physical address** with the **interface** or port to forward a frame to the address.
- It uses software to manage the bridge table and the forwarding process.
- It breaks collision domains (i.e. each port of a bridge is connected to a separate collision domain) but not broadcast domains (i.e. a bridge will forward a broadcast frame out all the active ports).
- Some bridges can also translate frames between different protocol types (e.g. token ring and Ethernet).
- It is hard to find any bridge in the market now. Vendors produce switches instead of

bridges.

4.6 A **switch** has the following characteristics:

- It is a multi-port bridge. It has a lot more ports than a bridge.
- It works at Layer 2 traditionally (**Layer 2 switching**). However, newer **multi-layered switches** can also work at upper layers to provide enhanced features, e.g. IP routing (**Layer 3 switching**), load-balancing by forwarding packets based on the TCP or UDP port numbers of the packets (**Layer 4 switching**), forwarding packets based on application layer information (**Layer 5-7 switching** or **Layer 7 switching**).
- It uses specialized hardware (Application Specific Integrated Circuits, **ASICs**) to perform switching and routing, which is more efficient than bridges and routers.
- It uses **Virtual LANs (VLANs)** to divide network devices into logical groups based on their functional, security, or other requirements, instead of their physical locations (details about VLAN can be found in Section 6). VLAN is not supported on bridges.

4.7 A **router** has the following characteristics:

- It works at the network layer.
- It connects similar or dissimilar networks. Each interface of a router is connected to a separate network.
- It routes datagrams based on the destination IP addresses (or other network layer protocol addresses) of the datagrams.
- It maintains a **routing table**. Each entry in the table maps a **destination network** with the **interface** or the **next hop router** to forward a datagram to the network using the shortest path.
- A routing table entry contains the following information:
 - The **network address** and **netmask** of the destination network.
 - The **exit interface** or the address of the **next hop router** to forward a datagram to the network.
 - The **metric** which denotes the "distance" to the network through this exit interface.
- It breaks both collision domains and broadcast domains (i.e. it does not forward broadcast and multicast traffic by default). Each interface is connected to a separate collision domain and broadcast domain.
- It can use access control lists (ACLs) to filter packets based on their network layer header information (e.g. source and destination IP addresses).
- It can provide connections between VLANs.
- It can provide Layer 2 bridging function if needed.
- It can provide quality of service (QoS) for specific types of network traffic.

4.8 A **routing table** can be maintained in two different ways:

- **Static routing** - routing table entries are static and can only be modified manually.
- **Dynamic routing** - different routers communicate with each other for routing information (e.g. a link is down, congested, etc.) using a **routing protocol** (e.g. RIP, OSPF, BGP, etc.). A router uses the information to calculate the shortest or most economical path to a destination network and update its routing table.

4.9 A **brouter** combines the functions of a bridge and a router. When it receives a packet, it first tries to route the packet. If it cannot determine the proper path, it tries to forward the packet based on the destination physical address.

4.10 A **gateway** works at the application layer. It is a device (or the software on a device) that connects two different environments. It translates messages between the two environments and controls the interactions between them. For example, an email-gateway can connect a Lotus Domino LAN-based email environment with the SMTP format Internet email environment.

5. LAN Segmentation & Switching

LAN Segmentation

5.1 In a **collision domain**, a frame sent by a device can cause collision with a frame sent by another device in the same collision domain. Moreover, a device can hear the frames destined for any device in the same collision domain.

5.2 In a **broadcast domain**, a broadcast frame sent by a device can be received by all other devices in the same broadcast domain.

5.3 A **LAN segment** or an Ethernet network segment consists of the devices connected with a coaxial cable or a hub. The devices are in the same collision domain.

5.4 **Ethernet congestion problem** occurs when too many devices are connected to the same Ethernet network segment, such that the high network bandwidth utilization increases the possibility of collision, which causes degradation of network performance.

5.5 **LAN segmentation** solves the congestion problem by breaking the network into separate segments or collision domains using bridges, switches or routers (but not hubs or

repeaters). LAN segmentation can reduce the number of collisions in the network and increase the total bandwidth of the network (e.g. 10 Mbps for one segment, 20 Mbps for two segments, 30 Mbps for three segments, and so on).

- 5.6 The **80/20 rule** should be used when designing how to segment a network, i.e. 80% or more data traffic should be on the local network segment while 20% or less data traffic should cross network segments.

LAN Switching

- 5.7 **LAN switching** (or **Layer 2 switching**) refers to the switching of a frame from the source computer to the destination computer across network segments. It consists of three major functions:

- **Address learning** - learning the MAC addresses of the connected devices to build the bridge table.
- **Forward and filter decision** - forwarding and filtering frames based on the bridge table entries and the bridge logic.
- **Loop avoidance** - avoiding network loop by using Spanning Tree Protocol (details about the protocol is outside the scope of this book).

- 5.8 A bridge or switch maintains a **forwarding table** (also known as **bridge table** or **MAC address table**) which maps **destination physical addresses** with the **interfaces** or **ports** to forward frames to the addresses.

- 5.9 A bridge or switch builds a bridge table by **learning** the MAC addresses of the connected devices. The process is as follows:

1. When a bridge is first powered on, the bridge table is empty.
2. The bridge listens to the incoming frames and examines the source MAC addresses of the frames. For example, if there is an incoming frame with a particular source MAC address received from a particular interface, and the bridge does not have an entry in its table for the MAC address, an entry will be created to associate the MAC address with the interface.
3. An entry will be removed from the bridge table if the bridge has not heard any message from the concerned host for a certain time period (e.g. 5 minutes).

- 5.10 A bridge or switch **forwards** or **filters** a frame based on the following logic:

1. If the destination MAC address of the frame is the broadcast address (i.e. FFFF.FFFF.FFFF) or a multicast address, the frame is forwarded out all interfaces, except the interface at which the frame is received.

2. If the destination MAC address is a unicast address and there is no associated entry in the bridge table, the frame is forwarded out all interfaces, except the interface at which the frame is received.
3. If there is an entry for the destination MAC address in the bridge table, and the associated interface is not the interface at which the frame is received, the frame is forwarded out that interface only.
4. Otherwise, drop the frame.

6. Virtual LAN (VLAN)

- 6.1 A **Virtual LAN (VLAN)** is a **broadcast domain** created based on the functional, security, or other requirements, instead of the physical locations of the devices, on a switch or across switches. With VLANs, a switch can group different interfaces into different broadcast domains. Without VLANs, all interfaces of a switch are in the same broadcast domain; switches connected with each other are also in the same broadcast domain, unless there is a router in between.
- 6.2 Different ports of a switch can be assigned to different VLANs. A VLAN can also span multiple switches (i.e. have members on multiple switches).
- 6.3 The advantages of implementing VLAN are:
- It can group devices based on the requirements other than their physical locations.
 - It breaks broadcast domains and increases network throughput.
 - It provides better security by separating devices into different VLANs.
 - Since each VLAN is a separate broadcast domain, devices in different VLANs cannot listen or respond to the broadcast traffic of each other.
 - Inter-VLAN communication can be controlled by configuring access control lists on the router or Layer 3 switch connecting the VLANs.
- 6.4 VLANs can be configured using one of the following two methods:
- **Static VLAN**
 - Assigning VLANs to switch ports based on the **port numbers**.
 - It is easier to set up and manage.
 - **Dynamic VLAN**
 - Assigning VLANs to switch ports based on the **MAC addresses** of the devices connected to the ports.
- 6.5 A **VLAN** is different from an **IP subnet** (details about IP subnet can be found in Chapter

4) in concept. However, there is a one-to-one relationship between a VLAN and an IP subnet. It means that devices in the same VLAN are also in the same IP subnet, devices in different VLANs are also in different IP subnets.

6.6 **Conventional switching** (i.e. **Layer 2 switching**) cannot switch frames across VLANs.

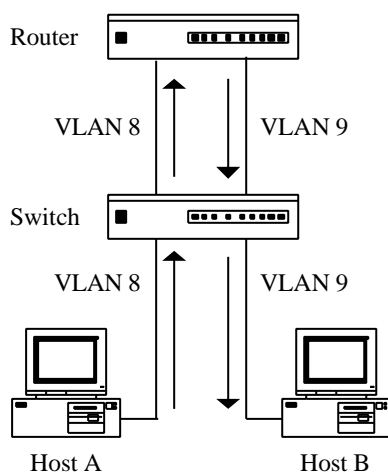
6.7 To forward packets between VLANs, a **router** or a **Layer 3 switch** is required.

6.8 There are two different types of links in a switched network:

- **Access link** - a link that is part of only one VLAN. Therefore, a port connected to an access link can be a member of only one VLAN.
- **Trunk link** - a link that connects switches or routers, and carries frames of different VLANs. Therefore, a port connected to a trunk link can be a member of multiple VLANs. All VLANs are configured on a trunk link by default.

6.9 A router can route traffic between different VLANs by having a physical interface connected to the switch for each VLAN. Each interface is connected to an **access link** of the switch. The default gateway of the hosts in each VLAN should be configured as the interface of the router connected to that VLAN.

6.10 For example, if Host A in VLAN 8 sends a packet to Host B in VLAN 9, the packet will be forwarded to the router's interface for VLAN 8 because it is the default gateway of Host A (and other hosts in VLAN 8). The router will then route the packet out the interface for VLAN 9 (the VLAN of Host B) based on IP routing (details about IP routing can be found in Chapter 4). The switch will then forward the packet to Host B.



6.11 If a router supports VLAN trunking, it can route traffic between different VLANs by

having only one physical interface connected to the switch. The interface should be connected to a **trunk link** of the switch carrying traffic for all the VLANs. This type of configuration is sometimes called "**router on a stick**".

6.12 A **Layer 3 switch** is a switch with routing features. It uses specialized hardware (Application Specific Integrated Circuits, ASICs) to route packets between VLANs or IP subnets. Therefore, it is more efficient than routers. Moreover, VLAN routing does not involve processing of the Layer 3 header of the packets.

7. Wireless LAN Technologies

Wireless LAN Basics

7.1 There are two types of **Wireless LAN (WLAN)**:

- **Ad hoc WLAN**
 - A purely wireless network.
 - Every device has a **wireless NIC** (e.g. PCI or PC Card add-on card, or USB adapter for providing wireless access). The devices communicate with each other without any access point.
 - Independent Basic Service Set (IBSS) refers to a group of wireless devices communicating in adhoc mode.
 - It is suitable for a few wireless devices to form a temporary workgroup network.
- **Infrastructure WLAN**
 - A WLAN which extends a wired network.
 - **Wireless access points (WAPs)** or **Access points (APs)** are the transceivers on a wired network that wireless devices communicate with. They act like switches to connect wireless devices to the wired network, and to the other wireless devices in the wireless network.
 - Basic Service Set (BSS) refers to a group of wireless devices communicating through a single wireless access point.
 - Extended Basic Service Set (EBSS) or Extended Service Set (ESS) refers to one or more interconnected BSSs sharing a common SSID.
 - It is suitable for a wireless network with a large number of devices, or the wireless devices need to communicate with wired networks.

7.2 There is a type of wireless access point that includes a built-in router for connecting wireless clients to the Internet. This type of device is known as **broadband router** or **wireless router**. It can also act as a DHCP server to assign private IP addresses to the

clients, and as a NAT server to perform port address translation between the global IP address (only one address) assigned by the ISP and the private IP addresses (multiple addresses, one for each client) assigned to the clients.

7.3 A wireless NIC has a radio antenna which acts as both the transmitter and receiver.

There are two main categories of antennas:

- **Omni-directional**
 - Point-to-multipoint (i.e. the power is dispersed in all directions).
 - The AP can be in any direction.
 - Shorter range than an equivalently rated directional antenna.
- **Directional** (also known as **Yagi**)
 - Point-to-point (i.e. the power is focused in one direction).
 - The direction to the AP should be aligned with the antenna.
 - Longer range than an equivalently rated omni-directional antenna.

7.4 **Antenna gain** is a measure of the effectiveness of a directional antenna in a given direction compared with an isotropic antenna (an antenna that radiates or receives equally in all directions). An antenna with a higher gain value can support a longer range.

7.5 In general, the gain of an antenna operating with a frequency below 1GHz is measured in decibel dipole (**dBd**), and the gain of an antenna operating above 1 GHz is measured in decibel isotropic (**dB*i***). dBd can be converted into dB*i* using this formula:

$$\text{dB}_i = \text{dB}_d + 2.2.$$

7.6 WLAN uses the frequency range of **2.4 - 5 GHz** of electromagnetic wave. It is based on the **IEEE 802.11** standards, which is also known as **Wi-Fi** (Wireless Fidelity). The IEEE 802.11 includes several standards:

Standard	Frequency	Modulation Techniques	Transmission rate	Max. Range (indoor)	Max. Range (outdoor)
IEEE 802.11	2.4 GHz	IR/FHSS/DSSS	1-2 Mbps	100m	450m
IEEE 802.11a	5 GHz	OFDM	54 Mbps	50m	300m
IEEE 802.11b	2.4 GHz	DSSS	11 Mbps	100m	450m
IEEE 802.11g	2.4 GHz	OFDM/DSSS	54 Mbps	100m	450m

*Remark:

- The actual range depends on the obstacles between the client and the access point (the more obstacles there are, e.g. walls, the more attenuated the signals become), and the interference from other wireless devices.
- The maximum data transmission rate is only available within limited distance from an access point

(typically 10m for 802.11a, and 30m for 802.11b/g for indoor). As the wireless device moves farther away from the access point, the transmission rate is reduced.

7.7 The first 802.11 specifications were introduced in 1997 and included three modulation methods for transmission in the unlicensed 2.4GHz band: infrared, FHSS, and DSSS. Only DSSS is supported by most wireless product vendors.

7.8 IEEE 802.11a and 802.11b are both introduced in 1999. However, they are incompatible with each other. 802.11a has the following advantages and disadvantages compared with 802.11b:

Advantages:

- Higher data transmission rate.
- Less interference since the 5GHz band is less heavily used than the 2.4GHz band.

Disadvantages:

- The higher carrier frequency restricts the use of 802.11a to almost line of sight (so that more APs are required) and shorter distance limit as it cannot penetrate as far as 802.11b.

7.9 802.11a products were released approximately two years after the 802.11b products because of the slow availability of the 5 GHz components. 802.11a was not popular because 802.11b had already been widely adopted, the cost of 802.11b equipment was lower, and the other disadvantages of 802.11a mentioned above.

7.10 IEEE 802.11g supports high data transmission rate, and is also backward compatible with 802.11b (e.g. a 802.11b NIC can work with an 802.11g access point at 802.11b speed). This standard is commonly used nowadays.

7.11 **Wi-Fi Alliance** is a non-profit industry trade association devoted to promoting the growth of WLAN. Their certification programs ensure the interoperability of WLAN products from different manufacturers.

7.12 The **802.11 physical layer** can use the following modulation techniques:

- Direct Sequence Spread Spectrum (DSSS).
- Frequency Hopping Spread Spectrum (FHSS).
- Orthogonal Frequency Division Multiplexing (OFDM).
- Infrared Pulse Modulation (IR).

7.13 The **802.11 data link layer** is based on CSMA/CA. Only one station can transmit in a WLAN at any one time. A station can reach another station with a distance limit of 30 -

100 m (for indoor) depending on the environment, e.g. number and structure of obstructions.

7.14 A **Service Set Identifier** (SSID) is a 32-character unique identifier that identifies a wireless network. It is also known as **Network Name**. The header of a packet sent over a WLAN contains the corresponding SSID.

7.15 **Association** is the process of establishing a wireless link between a client and an access point. **Re-association** takes place when a wireless client roams from one access point to another.

Wireless LAN Security

7.16 802.11b offers two authentication methods:

- **Open System Authentication** (OSA)
 - Encryption is not required. Negotiation and data transmission are in clear text.
 - A wireless device only needs to be configured with the correct SSID to gain access to the network.
 - It provides little security protection to the network because:
 - The SSID is stored as plain text in a packet.
 - Most access points have the default configuration of broadcasting their SSIDs so that wireless clients can browse and find them.
- **Shared Key Authentication** (SKA)
 - Encryption is required.
 - A wireless device must be configured with the required cryptographic key to gain access to the network.
 - Wired Equivalent Privacy (WEP) is used for authentication and encryption.

7.17 **Wired Equivalent Privacy** (WEP) is a security protocol defined in 802.11b. It provides:

- **Authentication** - CHAP type authentication (details about CHAP can be found in Chapter 6).
- **Data encryption** - RC4 encryption using a 40-bit or 104-bit secret shared key concatenated with a 24-bit initialization vector (IV) to create a 64-bit or 128-bit key.

It requires the access points and wireless clients to be configured with the same encryption key.

7.18 WEP is not very secure because of the following weaknesses:

- Static keys are used which are rarely changed by users.

- A weak implementation of the RC4 algorithm is used.
- The length of an initialization vector used is too short and the vector "wraps around" in a short period of time, resulting in repeated keys.

7.19 In October 2002, the Wi-Fi Alliance announced a new encryption solution called **Wi-Fi Protected Access (WPA)**, which supersedes WEP. It has the following characteristics:

- It is compatible with WEP. WEP-enabled hardware/software can be upgraded to support WPA.
- It includes both the Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms to provide dynamic key encryption and mutual authentication for wireless clients.
- It addresses the security weakness of WEP, e.g. the length of the IV has been increased from 24 bits to 48 bits, there is built-in key management mechanism for key generation and distribution, etc.

7.20 **IEEE 802.1x** is a port-based authentication framework. It allows different types of authentication methods to be used, e.g. RADIUS. It uses the Extensible Authentication Protocol (EAP) for message exchange during the authentication process.

7.21 A list of the security measures that should be implemented for a WLAN are listed below:

AP

- Change the default login name and password of the APs.
- Physically place the APs in the center of a building (to control the span of signals).

SSID

- Change the default SSID name of the network.
- Disable the broadcasting of SSID name.

MAC Address Filtering and other Access Controls

- Only allow wireless NICs of specific MAC addresses be connected to the APs, if the APs support this feature (MAC address filtering).
- Assign static IP addresses to the wireless clients and disable DHCP.
- Logically place the APs in a DMZ and use firewalls to control the traffic to/from the APs, e.g. by MAC addresses and IP addresses.
- Implement IEEE 802.1x authentication (e.g. RADIUS).

Encryption

- Enable WEP or WPA.
- Implement an additional layer of data encryption (e.g. VPN).

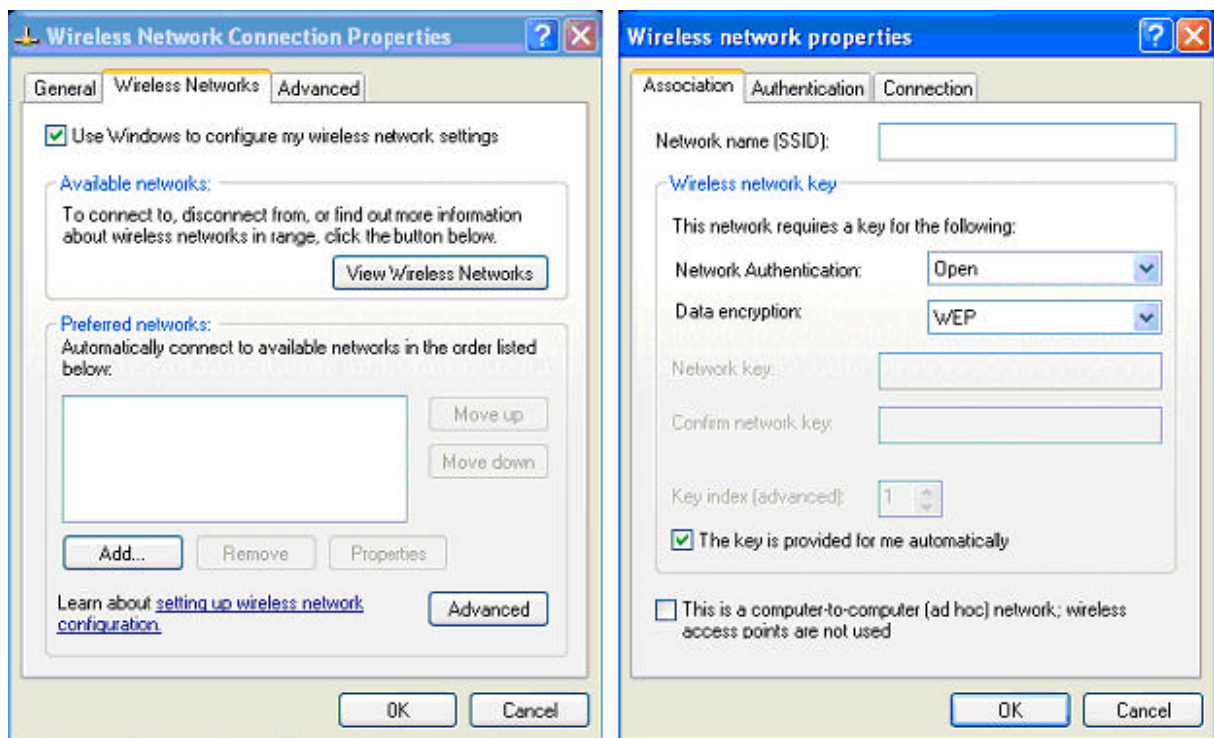
7.22 **War driving** means a hacker driving around with a laptop to identify APs, sniff wireless traffic, and attempt to gain unauthorized access to a wireless network through APs.

Configuring Wireless LAN

7.23 Windows XP requires the following configuration steps for connecting to a WLAN:

1. After you physically install the wireless NIC and boot the computer, the software required for configuring a wireless connection will be installed automatically.
2. Either open the "Wireless Network Setup Wizard" or the "Wireless Network Connection Properties" panel as follows:
 - **"Wireless Network Setup Wizard":**
 - a. Choose "Start" => "Control Panel" => "Wireless Network Setup Wizard".
 - **"Wireless Network Connection Properties" panel:**
 - a. Choose "Start" => "Control Panel" => "Network Connections".
Alternatively, you can open the "Network Connections" window by choosing "Start" => "All Programs" => "Accessories" => "Communications" => "Network Connections".
 - b. Right click the "Wireless Network Connection" icon and select "Properties" to open the "Wireless Network Connection Properties" panel => select the "Wireless Networks" tab.
 - c. From the list of preferred networks, i.e. all the wireless networks that the workstation has connected to before, open the "Wireless Network Properties" panel for the network to be connected as follows:
 - select the network to connect and click the "Properties" button; or
 - click the "Add" button to connect to a network that is not on the list.If there is more than one preferred network, the workstation will try to connect to the networks in the order listed.
3. Configure the following wireless network settings through the wizard or the "Wireless Network Properties" panel - "Association" tab:
 - **Network name** - SSID of the wireless network to connect.
 - **Network Authentication** method
 - Open System Authentication;
 - Shared Key Authentication;
 - WPA; or
 - WPA-PSK (WPA with pre-shared key).
 - **Data Encryption** method
 - Disabled or WEP (if Open System or Shared Key authentication method is used).
 - TKIP or AES (if WPA or WPA-PSK authentication method is used).
 - **Network Key**
 - If WPA-PSK authentication method is used, the key must be configured manually.

- If WPA authentication method is used, the key is provided by the AP automatically.
 - If WEP encryption method is used, the key can be configured manually or provided automatically.
 - Whether the workstation is connected to other wireless devices (**ad hoc WLAN**) or to an access point (**infrastructured WLAN**).
4. In the "Wireless Network Connection Properties" panel, you can also:
 - View all the wireless networks within range by clicking the "View Wireless Networks" button.
 - Choose not to use Windows XP to configure the wireless settings (some wireless NICs use their own external programs for the configuration).
 5. Configure the workstation for network access as discussed in Chapter 7.



7.24 Different models of wireless APs have different configuration procedures. However, the procedures are similar and typically include the following steps:

1. Configure a workstation such that it is in the same subnet as the AP. For example, if the AP has an IP address of 192.168.1.1 and subnet mask of 255.255.255.0, configure the workstation with an IP address of, says, 192.168.1.2 and subnet mask of 255.255.255.0.
2. Connect the workstation to the AP.
3. Typically, an AP can be configured through the web browser interface. On the workstation, open a web browser and access the AP through HTTP.

4. Once successfully access the AP's configuration menu through the browser, configure the following parameters of the AP:
 - SSID.
 - IP address and subnet mask of the AP customized for your LAN environment.
 - Operating mode - Access Point mode or Bridge mode (2 APs in the bridge mode can provide a wireless bridge between two wired network segments).
 - Password (for accessing the AP's configuration).
 - Wireless channel (for avoiding interference).
 - WEP - if it is enabled, the encryption key should also be configured.

Table of Contents of CompTIA Network+ Exam Notes

Chapter 1.	Introduction to Networking	1
1.	NETWORKING DEFINITIONS	1
2.	STANDARDS BODIES	2
3.	OPEN SYSTEM INTERCONNECT (OSI)	3
4.	TRANSMISSION CONTROL PROTOCOL / INTERNET PROTOCOL (TCP/IP)	7
5.	OTHER NETWORK PROTOCOL SUITES	10
6.	NETWORK COMMUNICATION CHARACTERISTICS	14
Chapter 2.	Network Types and Network Media	16
1.	NETWORK TYPES	16
2.	NETWORK MEDIA	18
3.	CABLE INSTALLATION AND TESTING TOOLS	26
4.	HIERARCHICAL NETWORK MODEL	27
Chapter 3.	LAN Technologies	29
1.	LAN MEDIA ACCESS	29
2.	LAN PROTOCOLS	32
3.	ETHERNET TECHNOLOGIES	34
4.	LAN DEVICES	38
5.	LAN SEGMENTATION & SWITCHING	41
6.	VIRTUAL LAN (VLAN)	43
7.	WIRELESS LAN TECHNOLOGIES	45
Chapter 4.	Fundamentals of TCP/IP - Part I	53
1.	INTRODUCTION	53
2.	IP HEADER	53
3.	IP ADDRESSING	55
4.	IP SUBNETTING	57
5.	IP ROUTING	59
6.	ROUTING PROTOCOLS	61
7.	CONSERVATION OF PUBLIC IP ADDRESSES	65
8.	ICMP FUNDAMENTALS	70
Chapter 5.	Fundamentals of TCP/IP - Part II	73
1.	TCP FUNDAMENTALS	73
2.	UDP FUNDAMENTALS	79

3.	DNS, WINS, AND DHCP	80
4.	CONFIGURING TCP/IP	85
5.	TCP/IP UTILITIES	89
Chapter 6.	WAN Technologies	103
1.	INTRODUCTION	103
2.	WAN DATA LINK PROTOCOLS	105
3.	PSTN AND DIAL-UP CONNECTION	107
4.	LEASED LINE CONNECTION	113
5.	INTEGRATED SERVICES DIGITAL NETWORK (ISDN)	113
6.	DIGITAL SUBSCRIBER LINE (DSL), CABLE MODEM, AND SATELLITE	116
7.	X.25, FRAME RELAY, AND ATM	119
Chapter 7.	Network Operating Systems	122
1.	INTRODUCTION	122
2.	MICROSOFT WINDOWS	122
3.	NOVELL NETWARE	128
4.	UNIX/LINUX	130
5.	MACINTOSH	131
6.	CONFIGURING WORKSTATION FOR NETWORK ACCESS	133
Chapter 8.	Network Security	136
1.	INTRODUCTION	136
2.	PHYSICAL SECURITY	137
3.	ACCESS CONTROL AND AUTHENTICATION	139
4.	FIREWALL	143
5.	ENCRYPTION AND VIRTUAL PRIVATE NETWORK (VPN)	147
6.	SYSTEM SECURITY EVALUATION	154
7.	INTRUSION AND DEFENSE TECHNIQUES	156
8.	OPERATION SECURITY	160
9.	DISASTER RECOVERY PLANNING	168
Chapter 9.	Network Troubleshooting	170
1.	TROUBLESHOOTING METHODOLOGY	170
2.	TROUBLESHOOTING TOOLS	172
3.	LOG FILES	174
4.	DOCUMENTATION	176

Appendix		178
1.	USEFUL WEBSITES	178
2.	IEEE 802 STANDARDS	179
3.	COMMONLY USED WELL-KNOWN TCP AND UDP PORTS	180

CompTIA Network+ Exam Notes - All you need to pass the exam

Copyright©2006 by the KP Lab Limited. All rights reserved. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher.

ISBN-13 978-988-97323-4-9
ISBN-10 988-97323-4-3
Publisher KP Lab Limited
Author K. Wan
Web Site www.kp-lab.com
e-mail kplab@pacific.net.hk

About the Author

K. Wan, MSc., CISSP, CCNP, CCSE, MCSE, MCDBA, SCSA, SCNA, SCJP, has more than ten years' experience in system and security administration on various computing platforms. He is currently an IT infrastructure and security manager working in Hong Kong.

IT Certification Examination Study Guides published by KP Lab:

1. CISSP Exam Notes
ISBN: 988-97323-1-9
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$19.99):
<http://www.kp-lab.com/cissp.htm>

2. CCNA 640-801 Exam Notes
ISBN: 988-97323-2-7
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$10.39):
<http://www.kp-lab.com/ccna.htm>

3. CCNP BSCI 642-801 Exam Notes
ISBN: 988-97323-3-5
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$14.95):
http://www.kp-lab.com/ccnp_bsci.htm

4. CompTIA Network+ Exam Notes
ISBN: 988-97323-4-3, 978-988-97323-4-9
Free Chapter:
<http://www.kp-lab.com/download.htm>
Full version (\$14.95):
http://www.kp-lab.com/comptia_network.htm