Chapter 10

Telecommunication Management Network (TMN)
International Telecommunication Union-Telecommunication (ITU-T)
Operations Support System (OSS)

Standard for TMN based on ISO network management which in turn is based on (CMIP) for protocol and (CMIS) for services.

TMN framework address:

- The management of quality of network elements
- Service management
- Business management.

Components of service management for TMN: (OAMP)

- Operations
- Administration
- Maintenance
- Provisioning

TMN have 2 methodologies:

- OMNI Point
- eTOM

Reason for TMN:

- Necessity for interoperability basis and need for management of more than just the network components.
- For Services, need to managed internal and external.
- For Business management needs to be addressed
- Networks / subnetworks need to be managed
- TMN joint effort by ITU-T and ISO

Operation Systems is a basic component of TMN:
TMN is built using the building blocks of the operations support system **and** It is used to control the network and network elements.
2 Example of Operation Systems that are used in the operation of telephone network and services:

- **Trunk test system:** Trunk is a logical connection between two switching nodes.
- **Traffic measurement system:** Traffic monitored at switch appearance and Call-blocking statistics obtained. (Importance of OAMP)

Traffic and call-blocking statistics provide data for planning.

TMN manage:

- **Data communication**: consists of LAN, bridges, gateways and hosts.
- **Telecommunication network**: consists of network elements of switching exchange and transmission systems.
  - Switching system include both analog and digital switches.

TMN conceptual model includes: (Components + Interfaces)

- **Components**
  - Customers
  - Service providers
  - Network
  - Operations support systems, OSSs
  - System operators / Workstation

- **Interfaces: (8 رسمة سلايد)**
  - Q3: is the interface between the operations system and the network element.
  - F: is the interface between the workstation and the operation system
  - X: used to exchange information between operations systems belongs to different TMNs.

TMN architecture:

- **Functional**
  - Functional modules or blocks (five function blocks:)
    1. MF → Mediation Function
    2. NEF → Network Element Function: Functions needed to support network elements; network elements themselves are not part of TMN (hubs, routers, switches, etc.).
       NM agent, MIB, and information for management (collision rate, packets dropped, etc.) are part of TMN
    3. OSF → Operations Systems Function: Functions performed by Operations systems: e.g., NMS, testing, accounting, trouble tracking.
    4. QAF → Q-Adapter Function: TMN non-compliant devices are connected to TMN-compliant system/network using QAF.
    5. WSF → Workstation Function
  - Reference points between modules: Function blocks connected by conceptual interfaces, called reference point

reference point designated by lower case letters (upper case letter for physical interfaces).

- **x:** Interface between operations systems that belong to different domains; e.g., interface between two NMSs belonging to two different domains
- **q3:** Interface between two OSFs (Functions performed by Operations Systems) in the same domain
- **qx:** Interface between mediation function such as RMON and agent in the network element
- **f:** Interface to the workstation

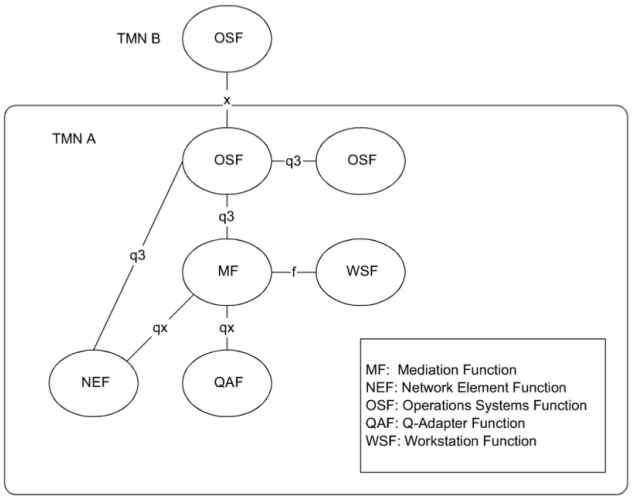


Figure 10.7 TMN Functional Architecture

- **Physical (**Have the same Five types of Function Architecture and Reference point with upper case letter**).**
  - Physical blocks
  - Physical interfaces between the blocks
- **Informational**
  - Information exchange between entities (managed objects and management system using distributed object-oriented approach).
  - Object oriented

TMN service management architecture: (presented as TMN layered architecture)

- Business management: **Top** layer, business management layer, it is concerned with managing communication business.
- Service management: Service management layer, concerned with managing the service provided by network service provider to customer or to another network service provider.
- Network management: **Third** layer is the network management layer, which manage the network. The network management functions in this layer would include bandwidth, performance, quality of service, end-end flow control, network congestion control.
- Element management: **Next** layer, the network element management layer, manages the network elements.
- Network element: **Lower** layer is the network element layer comprising network elements such as switches, bridges, transmission facilities.

TMN management services are classified into OSI system management functional areas, which are five OSI application function, they are:

- Fault
- Configuration
- Accounting
- Performance
- Security Functions

There are three forums that have actively promoted the implementation of TMN:

- ATM forum (now IP/MPLS Forum)
- NMF (Known as Network Management Forum)
- TM forum

implementation of TMN have 2 examples:

Example1: OMNIPoint

- Is An example under NMF.
- which stands for Open Management Interoperability Point.
- The objective is to help companies implement management standards across a wide range of suppliers' equipment.

Example 2: eTOM (Enhanced Telecom Operations)

- Developed by TM (Tele management forum)
- Aimed to align technology with real business
- An important goal of the TM Forum is to automate end-to-end the operations that enable delivery of "information, communication and entertainment services,"

Difference between TMN and eTOM:

- **TMN:** approaches is that the former has been developed starting from networks and network equipment (bottom up). AND management functional areas referred to as FCAPS (fault, configuration, accounting, performance and security).
- **eTOM:** is a top-down approach. AND referred to as FAB (fulfilment, assurance and billing).

eTOM-to-TMN mapping of functions

- Fulfillment Configuration
- Assurance Fault Performance
- Billing Accounting

Chapter 11

(ملاحظة تم إضافة المواضيع الجانبية فقط، المواضيع المرتبطة قد سبق وعملت لها خريطتين ذهنيتين تلقونهم في نفس المجلد)

Event Correlation Techniques:

- **Basic elements**
  - Detection and filtering of events
  - Correlation of observed events using ARTIfiCIAL Intelligence
  - Localize the source of the problem
  - Identify the cause of the problem
- **Techniques**
  - Rule-based reasoning
  - Model-based reasoning
  - Case-based reasoning
  - Codebook correlation model
  - State transition graph model
  - Finite state machine model

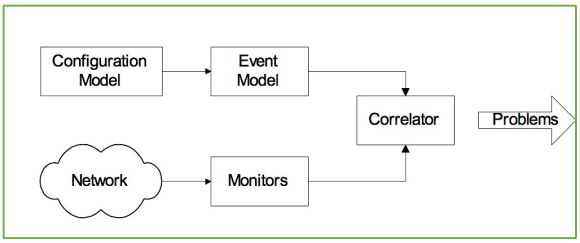
Traffic Flow Measurement Network Characterization:

Four levels defined by IETF (RFC 2063):

1. International Backbones / National
2. Regional / Midlevel
3. Stub / Enterprise
4. End-Systems / Hosts

Three measurement entities:

1. **Meters** gather data and build tables
2. **Meter readers** collect data from meters
3. **Managers** oversee the operation



Codebook Correlation Model: Generic Architecture:

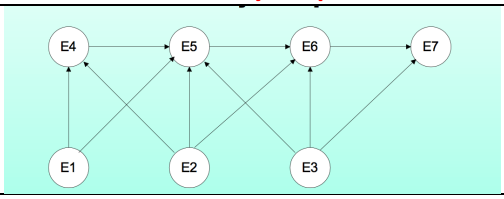
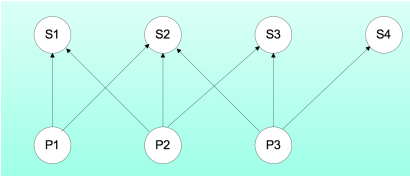
- **Monitors** capture alarm events.
- **Configuration model** contains the configuration of the network.
- **Event model** represents events and their causal relationships.
- **Correlator** correlates alarm events with event model and determines the problem that caused the events.

Codebook Approach:

- Correlation algorithms based upon coding approach to even correlation
- Problem events viewed as messages generated by a system and encoded in sets of alarms
- Correlator decodes the problem messages to identify the problems

Two phases of codebook Approach:

1. Codebook selection phase: Problems to be monitored identified and the symptoms they generate are associated with the problem. This generates codebook (problem- symptom matrix)
2. Correlator compares alarm events with codebook and identifies the problem.

Causality Graph	Labeled Causality Graph
	
• Each node is an event • An event may cause other events • Directed edges start at a causing event and • terminate at a resulting event • Picture causing events as problems and • resulting events as symptoms	• Ps are problems and Ss are symptoms • P1 causes S1 and S2 • Note directed edge from S1 to S2 removed; S2 is caused directly or indirectly (via S1) by P1 • S2 could also be caused by either P2 or P3
شرح الرسمة: هنا الرسمة تحدد لي البروبلم. كل نود طالع منها اسهم و مو داخل عليها اسهم هي عباره عن problems. وكل نود داخل عليها اسهم و طالع منها اسهم بشرط ان تكون اسهم داخل عليها تكون عباره عن symptoms.	هنا الرسمة مشابهه ل Causality Graph لكن النود الثلاث الي تحت تمثل لي problems والنود الأربع الي فوق تمثل لي symptoms. فيتم تمثيلهم ب P و S. والأسهم الي تكون بين ال S و S ثانية مو مهمه، المهم الي تكون بين P و S.

Codebook:

- Codebook is problem-symptom matrix
- It is derived from causality graph after removing directed edges of propagation of symptoms
- Number of symptoms => number of problems
- 2 rows are adequate to uniquely identify 3 problems

Correlation Matrix is reduced codebook

Correlation graph is derived from correlation matrix

Codebook Enhancements:

- Codebook described so far assumes Hamming distance of 1 for uniqueness
- Noise affects accuracy
- Increase Hamming distance to >1
- Probability of a problem causing a symptom assumed as 1. It can be made Si = Pr(Pj) to be more realistic

State Transition Model:

- Used in Seagate's NerveCenter correlation system
- Integrated in NMS, such as OpenView
- Used to determine the status of a node

Finite State Machine Model:

- Finite state machine model is a passive system; state transition graph model is an active system
- An observer agent is present in each node and reports abnormalities, such as a Web agent
- A central system correlates events reported by the agents
- Failure is detected by a node entering an illegal state

Secure Communication Network:

- Firewall secures traffic in and out of Network A
- Security breach could occur by intercepting the message going from B to A, even if B has permission to access Network A
- Most systems implement authentication with user id and password
- Authorization is by establishment of accounts

Packet Filtering Firewall:

Uses protocol specific criteria at **DLC**, network, and transport layers.

- In the OSI networking model, Data Link Control (DLC) is the service provided by the data link layer.

- Implemented in routers - called screening router or packet-filtering routers
- Filtering parameters:
  - Source and/or destination IP address
  - Source and/or destination TCP/UDP port address, such as ftp port 21
- Multistage screening - address and protocol
- Works best when rules are simple

Application Level Gateway:

- Firewalls 1 and 2 route traffic only from and to the secured LAN
- Secured LAN is gateway LAN
- Behavior of application gateway dependent on the application
- FTP traffic stored and forwarded after validation
- TELNET hosts validated for the session and then direct communication established

Cryptography:

"Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. It includes encrypting a message by its sender and decrypting it by its destination"

- Secure communication requires:
  - Integrity protection: ensuring that the message
  - Authentication validation: ensures the originator
- Security threats:
  - Modification of information
  - Masquerade
  - Message stream modification
  - Disclosure is not tampered with identification
- Hardware and software solutions for security threats
- Most secure communication is software based

Secret Key Cryptography	Public Key Cryptography
• Caesar cipher: each letter replaced by another letter, which is three letters behind in the alphabet ➢ Maximum of 26 attempts to decode Caesar cipher • Monoalphabetic cipher: Replace a letter with another randomly chosen; Maximum attempts to decode 26! • One secret key is needed between each pair • Two standard algorithms for secret key: ○ DES (Data Encryption Standard): ○ 64-bit message blocks and 56-bit key ○ IDEA (International Data Encryption Algorithm): ○ 64-bit message blocks and 128-bit key • Message block derived using CBC (Cipher Block Chaining) • Principle-based on rearranging the blocks several times based on predetermined algorithm and secret key **A cipher =** a secret or disguised way of writing; a code; the resulting message of the encryption.	• Asymmetric cryptography - public and private key • Public key is distributed by the receiver to the senders to encrypt the message. • Private key is used by receiver to decode ciphertext • Mailbox analogy • Commonly used public key is RSA (Rivest, Shamir, and Adleman); 512-bit key, variable block size • RSA less efficient than DES and IDEA; used to encrypt secret key

Message Digest:

- Message digest is a cryptographic hash algorithm added to a message
- One-way function
- Analogy with CRC
- If the message is tampered with, the message digest at the receiving end fails to validate
- MD5 (used in SNMPv3) commonly used MD
- MD5 takes a message of arbitrary length (32- byte) blocks and generates 128-bit message digest
- SHS (Secure Hash Standard) message digest proposed by NIST handles 264 bits and generates 160-bit output

Digital Signature:

Why do we need digital signature?

- Principle reverse of public key
- Signature created using private key and validated using public key
- Digital signature is a message digest generated from plaintext and private key by a hashing algorithm
- Digital signature is concatenated with the plaintext and encrypted using public key

Ticket-Granting System:

- Used in client/server authentication system
- Kerberos developed by MIT
- **Steps:**
  - User logs on to client workstation
  - Login request sent to authentication server
  - AS checks ACL, grants encrypted ticket to client
  - Client obtains from TGS service-granting ticket and session key
  - Application Server validates ticket and session key, and then provides service

SNMPv3 Security:

- Authentication key equivalent to DEK in PEM or private key in PGP
- Authentication key generated using user password and SNMP engine id
- Authentication key may be used to encrypt message
- USM prepares the whole message including scoped PDU
- HMAC, equivalent of signature in PEM and PGP, generated using authentication key and the whole message
- Authentication module provided with authentication key and HMAC to process incoming message

In **cryptography**, a **keyed-hash message authentication code(HMAC)** is a specific type of **message authentication code(MAC)** involving a **cryptographic hash function** (hence the 'H') in combination with a secret **cryptographic key**.

Virus Attacks:

- **Executable programs that make copies and insert them into other programs**
- Attack hosts and routers
- Attack infects boot track, compromises cpu, floods network traffic, etc.
- Prevention is by identifying the pattern of the virus and implementing protection in virus checkers

Chapter 12

Broadband WAN segment:

- IP (has been dealt with earlier)
- ATM
- MPLS
- Optical and MAN feeder network

ATM	MPLS	Optical and MAN feeder network
• Virtual path–virtual circuit (VP-VC) operation • Real-time and non-real-time function for broadband service • ATM as public and private switched networks • Emulated LAN configuration • ATM management: M1, M2, M3, and M4 interfaces • ATM digital exchange interface management	• Possesses rich features of IP and good performance of ATM • Basic principles of label switching • Label switched path, LSP • Traffic engineering • MPLS OAM • Service level management • MPLS MIBs • MPLS TE MIBs • MPLS example	• SONET-based MAN • SONET transport hierarchy • SDH and (D)WDM network • SDH management • WDM management

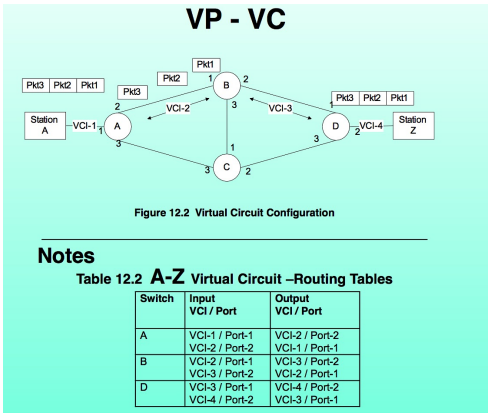
Broadband Services:

- **Broadband Integrated Services Digital Network (BISDN)** a.k.a broadband network
  - allow transfer of: Voice, video, and data services
  - define: Transport protocol and medium
- **(Basic) Integrated Services Digital Network (ISDN)** (The early form of ISDN a.k.a narrowband ISDN)
  - It consists of two basic channels: B-channels, 56-kilobaud rate each, combined with an 8-kilobaud signaling channel, D-channel. Together, they are referred to as **2B + D**
- **WAN**
  - ATM (Asynchronous Transfer Mode) Cell-based Technology
  - SONET (the Synchronous Optical Network – **American standard**)
    - OC-1 /STS (Optical Carrier-1/Synchronous Transport Signal), which is 51.84 Mbps.
  - SDH (the Synchronous Digital Hierarchy – **international standard**) **IS** a standard technology for synchronous data transmission on optical media.
  - MPLS (Multiprotocol Label Switching).
- **LAN**
  - ATM LAN Emulation
    - Emulate = To imitate the function of (another system), as by modifications to hardware or software that allow the imitating system to accept the same data, execute the same programs, and achieve the same results as the imitated system.
      - LAN emulation (LE or LANE)

The services provided by ATM differ in three ways:

1. ATM **is connection oriented**.
2. ATM **makes one-to-one connection**
3. a LAN MAC address is dedicated to the **physical network interface card** and is independent of network topology.

- **Access Technology**
  - Cable modem used HFC (Hybrid fiber coax)
  - DSL (digital subscriber line)
  - Wireless
- **Access Networks**
  - OC-n/STS ((Optical Carrier-n Synchronous Transport Signal)
  - HFC, xDSL and Fixed Wireless to residence
  - Limited mobile wireless technology



ATM Technology (~~مهم~~)

- **ATM technology based on:**
  - VP (Virtual path)/ VC (Virtual circuit)
  - Fixed packet size or cell
  - Small packet size (53 bytes)
  - Statistical multiplexing
  - Integrated services
  - After initial set up, latency is reduced
  - Variable bit rate
  - Simultaneous real- and non-real time traffic

VP - VC

- All packets take the same path and arrive in the same sequence in virtual circuit
- Packets in a session take the same path in VP/VC
- After initial set up, latency is reduced
- VCI= Virtual Circuit Identifier

ATM LAN Emulation (LANE)

- **Difference** between ATM and Ethernet
  - ATM is connection-oriented and Ethernet is connection less.
  - ATM makes one-to-one connection
  - ATM 20-byte addressing scheme and Ethernet is 6-byte MAC address
- LANE emulates services of a traditional LAN

ATM WAN Reference Model

- WAN service provided by public service providers
- Private networks use public WAN facilities
- Management functions (OAMP)
  - Operations • Administration • Maintenance • Provisioning
- Public and private User Network Interface (UNI) define user interfaces

ATM WAN Management

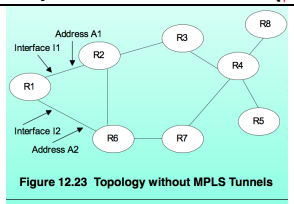
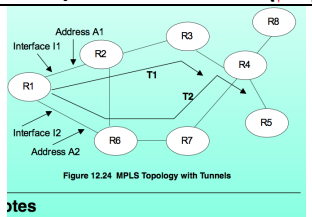
- Management interface architecture defined by ATM Forum
- Public and private NMS responsible to manage respective domains
- OSI has defined **five management interfaces:**
  - Interface between private NMS and end user
  - Interface between private NMS and network
  - Interface between private NMS and public NMS
  - Interface between public NMS and network
  - Interface between public NMSs

Simplified MPLS Network

- MPLS combines
  - Richness of IP
  - Performance of ATM
- FEC (forward equivalent classes) assigned at the ingress router and encoded in the label
- Label is removed at the egress router and original protocol packet is sent out

IP Network

- FEC (Forward Equivalent Class) decides the port for the next hop
- Packets with the same FEC are indistinguishable and sent to the same port
- FEC determination is complex and done at each node
- This leads to low performance (compare with ATM VP-VC achieving high performance)

MPLS / IP without Tunnel (ﷺ)	MPLS / IP with Tunnels (ﷺ)
 Figure 12.23 Topology without MPLS Tunnels **lotes** Table 12.12 R1 Routing Table without Tunnel Dest | Output Interface | Next Hop | Metric 2.2.2.2 | I1 | 2.2.2.2 | 1 3.3.3.3 | I1 | 2.2.2.2 | 2 4.4.4.4 | I1 | 2.2.2.2 | 3 I2 | 6.6.6.6 | 3 5.5.5.5 | I1 | 2.2.2.2 | 4 I2 | 6.6.6.6 | 4 6.6.6.6 | I2 | 6.6.6.6 | 1 7.7.7.7 | I2 | 6.6.6.6 | 2 8.8.8.8 | I1 | 2.2.2.2 | 4 I2 | 6.6.6.6 | 4	 Figure 12.24 MPLS Topology with Tunnels **otes** Table 12.13 R1 Routing Table with Tunnel Dest | 0 Intf | Next Hop | Metric 2.2.2.2 | I1 | 2.2.2.2 | 1 3.3.3.3 | I1 | 2.2.2.2 | 2 4.4.4.4 | T1 | 4.4.4.4 | 3 /1 5.5.5.5 | T2 | 5.5.5.5 | 4/1 6.6.6.6 | I2 | 6.6.6.6 | 1 7.7.7.7 | I2 | 6.6.6.6 | 2 8.8.8.8 | T1 | 4.4.4.4 | 4/2
• the IP addresses of the routers are designated as i.i.i.i for each router Ri. • Table shows the output interface (logical port) and next hop for packets emanating from R1 to Ri. • The last column in the table shows the metric of the number of hops from R1 to the destination router. • The paths are chosen using IGP. For example, there are two choices for the label- switched path (LSP) from R1 to R4, both of which are shown in Table 12.12. The two paths are R1–R2–R3–R4 and R1–R6–R7–R4. They both have the same metric of 3 hops.	• The LSRs (label- switched path) R4 and R5 are directly reached from R1 through tunneling. The transit time delay is low and the throughput is higher as the intermediate routers in the tunnel behave as pass through. • For the case of an LSP from R1 to R4, the corresponding metrics are 3 and 1 ➢ (out of the logical port L1 and has the next hop as R4- one is direct using tunneling and the other is without tunneling.) • For the case of an LSP from R1 to R5, the corresponding metrics are 4 and 1

MPLS-TE

- Traffic Engineering (TE): Optimization of performance
- Overlay over inadequate IGP:

• Constrained-base routing at VC level • VC paths • Path compression
• Call admission control • Traffic shaping and policing • VC survivability

Label Switching Router (LSR)

- MPLS router called Label Switching Rouer (LSR)
- End-to-end MPLS path called Label Switching Path (LSP)
- IGP extended to include MPLS-TE
- Route set up by RSVP-TE
- Control and data planes separated in MPLS
- VoIP handled using SIP (Session Initiation Protocol)

MPLS Label is:

- Short and fixed length – 32 bits
- FEC locally significant identifier
- Label assigned by the downstream router
- Label is "shimmed" between layers 2 and 3 headers

MPLS OAMP Management

- Data and control planes are separate in MPLS, (Data and control planes = Data and control channel)
- OAM packets travel the data path; OAM packets follow the data path (operations, administration, and maintenance)
- The MPLS layer can be visualized as the layer positioned between layers 2 and 3 and hence OAM of MPLS needs to address both networks, namely ATM/MPLS and IP/MPLS.
- Basic Tools
  - LSP connectivity verification (! End-to-end MPLS path called Label Switching Path)
  - LSP ping • LSP traceroute
- Fault management
- Configuration management
- Performance management

Fault Management of LSP

- LSP Fault scenarios:
  - Simple loss of connection
  - Misconnection
  - Swapped connection
  - Mismerging
  - Loop/unintended replication
- Detection of LSP fault using
  - connectivity verification (CV) – ITU-T
  - Bidirectional forwarding detection (BFD) - IETF

LSP Traceroute

- Similar to IP traceroute
- Hop-by-hop fault localization as well as path tracing
- Packet sent to control plane of each transit LSR
- Transit LSR validates LSP
- Validates control plane against data plane of the LSR

BFD

- Uses LSP-ping echo - response to detect data plane failure in LSP
- Helpful to detect failures in the data plane when the control plane is functional and data plane is not.
- Establishes session between ingress and egress LSRs
- Fast and low overhead detection between adjacent NEs
- BFD fault detection interval should be longer than switching time in the fast-reroute LSP.

SDH Management

- ITU-T G Series documentation
  - Transmission Systems and Media
  - Digital Systems and Networks
  - Digital Terminal Equipments
- G.774 SDH
  - Management Information Model
  - OAM
  - Data Communication Channels (DCCs)
- G.784 Element Management Functions (EMFs)
- G.831 Management capabilities of transport networks

SDH Data Communication Channels (DCC**)**

- G.774 specifies 3 modes of management for DCCs
  - IP-only stack use PPP as data link
  - OSI-only use LAP-D as data link
  - Dual (IP + OSI) stack PPP or LAP-D with tunneling to communicate between stacks

SDH Element Management Functions

- G.784 specs equipment management functions (EMF)

• Fault management • Performance management • Configuration management

- Two DCC channels
  - DCCM forwards over the multiplex sections: behaves as backbone network
  - DCCR (and LAN) forwards data to regenerators: interconnects backbone to equipment
  - DCCM and DCCR carry independent management applications

SDH Fault Management

- Alarm messages called" defects"
- Error messages called "anomalies"

SDH Performance Management

- Four commonly used parameters:

• Errored seconds (ES) • Severely errored seconds(SES)
• Background block error (BBE) • Unavailable seconds (UAS)

Chapter 13

Broadband Access Networks

- Access network between WAN and home network
- Four access network technologies:
  - **Cable** popular in North America
  - **ADSL** more extensively deployed elsewhere in the world
  - **Wireless**:
    - Fixed: MMDS, LMDS, and WiMax
    - Mobile: CDMA, GPRS
  - **PON** on fiber medium
- OC-n an extension of WAN for enterprise

Cable Access Network

- CM (Cable Modem) technology, also known as HFC (Hybrid fiber-coaxial) technology
- Head end:
  - Signals from multiple sources are multiplexed and up-converted from an electrical (radio frequency (RF)) to an optical signal
  - Frequency conversion for local signal
- Traffic Flow:
  - Downstream: Head end to NIU
  - Upstream: NIU to head end
- Network interface device (NID) / unit (NIU): Demarcation point between customer network and service provider networks
- Cable modem: RF signals voice-over-IP, video and digital data in general

Comparative Speeds

- The broadband cable access system with the CM can process data at a much faster rate than a conventional telephone modem or integrated services digital network (ISDN).

Telephone Modem 28.8 kbps	6 - 8 minutes
ISDN 64 kbps	1 -1.5 minutes
Cable Modem 10 Mbps	Approximately 1 second

Cable Access Network Technology

- Broadband 2-way cable access network
- Asymmetric bandwidth allocation for 2-way communication
- **Transmission Mode (مهم)**
  - Downstream: TDM broadcast mode
  - Upstream: TDMA / S-CDMA
    - Time-division multiplexing (TDM) is a method of putting multiple data streams in a single signal by separating the signal into many segments, each having a very short duration.
    - Time division multiple access (TDMA) is a channel access method for shared medium networks.
- RF spread-spectrum that carries multiple signals over HFC
- RF spectrum allocation to carry multimedia services - voice, video, and data

Cable Access Network

- Single physical medium, 2 logical data streams
- Downstream 6 MHz (North American) / 8 MHz (Europe, Asia) channels
- Upstream Variable speed channels 160 kbps to 5.2 Mbps
- Downstream TDM broadcast mode
- Upstream TDMA in DOCSIS 1.0 and 1.1
- Upstream S-CDMA in DOCSIS 2.0
  - DOCSIS: Data Over Cable Service Interface Specification.

Digital-to-Analog Encoding

- **bit rate:** The bit rate is the number of bits per second that traverses the medium
- **symbol (baud) rate:** The baud rate is the signal units/symbols per second • number of levels n = 2^k; k..number of bits per symbol;
- bit rate = symbol rate x k

Modulation Schemes (مهم)

- Different modulation techniques support different capabilities.
- the more common modulation techniques used are quadrature phase shift keying (QPSK) and quadrature amplitude modulation (QAM).
- Basic modulation techniques
  - ASK (Amplitude Shift Keying)
  - FSK (Frequency Shift Keying)
  - PSK (Phase Shift Keying)
- Cable technology uses

QPSK (Quadrature Phase Shift Keying)	**QAM** (Quadrature Amplitude Modulation) (16 levels — 4bits)
• Four levels (00, 01, 10, 11) encodable on 2 bits • Relatively insensitive to noise • Used for low-band upstream • 8 MHz channel: 8x2=16 Mbps	• Combination of AM and PM • 16-QAM=8PMx 2AMor4PMx4AM • Used for higher-band downstream • 8 MHz channel 8x4=32 Mbps

DSL Access Technology

- Why is DSL attractive?
  - The main motivating factor to employ xDSL (x digital subscriber line) for access technology in multimedia services is the pre-existence of local loop facilities to most households.

DSL Limitations (المحددات الي تخليني استخدم الدسل)

- local loop with no direct copper to the house
  - the **local loop** is the physical link or circuit that connects from the demarcation point of the customer premises to the edge of the common carrier or telecommunications service provider's network.
- Loaded coils (used to increase analog distance) in local loop cannot carry digital signal
  - a **coil** used to provide additional inductance in an electric circuit in order to reduce distortion and attenuation of transmitted signals or to reduce the resonant frequency of an aerial
- Operating company inventory dated (administrative issue)

ADSL Network

- **ADSL** (Asymmetric Digital Subscriber Line)
- ATU-C (ADSL transmission unit - central office)
- ATU-R (ADSL transmission unit - remote/residence)
- Splitter separates voice and data

xDSL Technologies

Table 13.8 DSL Technologies

Name	Meaning	Max Data Rate*	Mode	Cable	Applications
ADSL / ADSL2 / ADSL2+	Asymmetric Digital Subscriber Line	7/12/24 Mbps 0.8/1/1 Mbps	Down Up	1-pair	Most common type

There are 2 schemas to spreading upstream and downstream frequency band:

1. **FDM** (frequency division multiplexing)
   - **POTS** (Plain old telephone service)
2. **Echo cancellation** separates upstream and downstream signals

Modulation Schemes (بالنسبة للاب ستريم و الداون ستريم)

- Carrierless amplitude phase (CAP) modulation
- Discrete MultiTone modulation (DMT): 4kHz tones
- Both CAP and DMT are QAM-based
- **DMT outperforms CAP: (مهم)**
  - Higher downstream throughput > 4 times
  - Higher upstream throughput > 10
  - Rate adaptive
  - Ongoing active monitoring
  - Maximum loop variation coverage
  - Standard and hence interoperable

DSL / Broadband Forum

- ADSL (now Broadband) Forum is an industry consortium formed to:
  - Achieve interoperability
  - Accelerate DSL implementation
  - Address end-to-end system operation
  - Security
  - Management
- 3 sets of complementary standards adopted
  - ITU-T standards
    - G.992.x • G.997.x • T1-413 (ANSI)
  - Forum Standards
    - Technical reports TR-xxx
  - IETF standards
    - RFC xxxx (الاكسات تعبر عن ارقام)

VDSL Network

- Used in FTTN configuration
  - **Fiber to the node (FTTN)** is one of several options for providing cable telecommunications services to multiple destinations.
  - helps to provide broadband connection and other data services through a common network box, which is often called a node.
  - may also be called fiber to the neighborhood.
- Asymmetric band allocation (similar to ADSL)
- Fiber carries multiple channels to ONU (Optical Network Unit)
- Channels demultiplexed at ONU and carried to customer premises on multiple twisted pairs
- Shorter distance of multiple twisted pairs
- Higher data rate: 55.2 Mbps downstream and 2.3 Mbps upstream

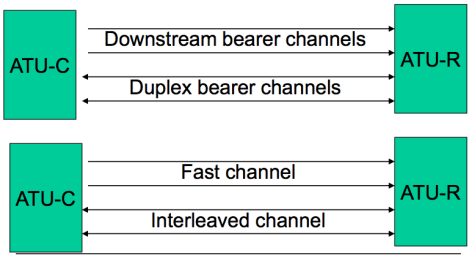
- ADSL Asynchronous Digital Subscriber Line
- ATM Asynchronous Transfer Mode STM Synchronous Transfer Mode
- TE Terminal Equipment OS Operations System
- PDN Premises Distribution Network SM Service Module

Transport Modes

- Synchronous transport mode (STM)
  - Bit synchronous transmission (T1/E1)
- End-to-end packet mode
  - Used for SOHO (IP packets)
- ATM / STM
  - ATM WAN (Public network) and STM access network
- ATM / Packet
  - ATM WAN and packet access network (IP)
- End-to-end ATM

ADSL Channeling Schemes

- **Transport bearer channels**
  - Seven AS downstream channels
    - multiples (1-, 2-, 3- or 4-) T1 rate of 1.536 Mbps
  - Three LS duplex channels
    - 160, 384, and 576 Kbps
- **Buffering scheme**
  - Fast channel: uses fast buffers for real-time data
  - Interleaved channel: used for non-real-time data
  - Both fast and interleaved channels carried on the same physical channel



ADSL management

- ADSL network management deals with parameters, operations, and protocols associated with configuration, fault, and performance management.

- Management of physical layer involves:
  - Physical channel
  - Fast channel
  - Interleaved channel
- Management of type of line encoding
  - DMT
  - CAP

Signal Power and Data Rate Management

- Five levels of noise margin
  1. Maximum noise margin
  2. Upshift noise margin
  3. Target noise margin
  4. Downshift noise margin
  5. Minimum noise margin
- Signal power controlled by noise margin
- Data rate: Increase or decrease based on threshold margins
- Data rate adaptation modes: Manual (1), automatic at start-up (2), and dynamic (3)

Fault Management For ADSL

- Failure indication of physical channel by NMS
- Failure indication of logical channels
- Failure indication of ATU-C/R
- Self-test of ATU-C/R as per T1.413
- Noise margin threshold alarms
- Rate change due to noise margin

Performance Management For ADSL

- Line attenuation
- Noise margin
- Output power
- Data rate
- Data integrity check
- Interleave channel delay
- Error statistics

ADSL Profiles Management

- Configuration profile

- (Configuration of ADSL lines in an ADSL system) Mode I - Dynamic **AND** Mode II - Static
- Performance profile
- Alarm profile
- Traps
  - Generic
  - Loss of frame
  - Loss of signal
  - Loss of power
  - Error-second threshold
  - Data rate change
  - Loss of link
  - ATU-C initialization failure

ADSL2 and ADSL2+

- Rate and reach Improvements
- **ADSL** Speed Downstream/Upstream 1/.256 Mbps
- **ADSL2** Standard G.992.3 July 2002
- ADSL2 Lite Standard G.992.4 July 2002
  - Speed Downstream/Upstream 12/1 Mbps
- **ADSL2+** Standard G.992.5 January 2003
  - Speed Downstream/Upstream 24/2 Mbps
- Other Major Enhancements
  - Diagnostics
  - Power enhancements
  - Rate adaptation
  - Bonding for higher data rates
  - Channelization and Channelized Voice-over DSL (CVoDSL)
- Additional Benefits
  - Improved interoperability
  - Fast startup
  - All-Digital Mode
  - Support of packet-based services

Other ADSL2 Enhancements

- Diagnostics by use of enhanced trans receivers
  - Line noise
  - Loop attenuation
  - SNR (Signal-to-Noise ratio)
- Improved interoperability due to initialization of state machine
- Fast startup
- Transmission of ADSL data in the voice bandwidth
- Ethernet over ADSL2

Passive Optical Network

- Fiber Medium
- No active elements in the transmission medium
- Passive elements in the fiber medium
  - Beam splitter – Lossy
  - Wavelength Division Multiplexer (WDM)

3 deployment configurations for PON:

Dedicated fiber	EPON	WDM
• Dedicated fiber from OLT to each ONU • ONU function similar to ONU in cable access network • One-way in each fiber / Dual wavelength fiber for 2-way • Expensive configuration	• Shared optical fiber from OLT to power splitter / combiner • Twisted pair or Cat-x cable from splitter / combiner to ONU • Modified Ethernet MAC protocol for EFM (Ethernet First Mile) • Downstream TDM and upstream TDMA • MIB specified only for EPON	Shared single fiber from OLT to WDM. wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e.,colors) of laser light. • DWDM (Dense WDM) special case of WDM.

Chapter 14

Wired & Wireless Broadband Networks

Wired/ Wireless technologies for:

1. WAN 2. Access Network 3. Customer premises network

Wireless Broadband Networks

The application of wireless technology can be grouped in 3 categories:

- Access Networks
  - MAN a.k.a. WiMax (Metropolitan Area Network)
- Wireless LAN (WLAN)
- Personal Area Network (PAN)

Outdoor Propagation

- Adverse Characteristics:
  - Attenuation
  - Dispersion: Frequency and Phase (independent of refractive index)
  - Dispersion due to refractive index
  - Decreasing signal strength due to beam pattern
  - Water absorption
  - Fading: short and long
    - **Fading:** A gradual loss of strength, or a slow disappearance.
  - Doppler effect
    - **Doppler effect**: A change in the observed frequency of a wave, as of sound or light, with the frequency increasing when the source and observer approach each other and decreasing when they move apart.

isotropic: (of an object or substance) having a physical property that has the same value when measured in different directions.

Non-Isotropic Propagation

- $P_R = P_T G_T G_R (\lambda/4d)2$
  - P_R = Received power
  - P_T = Transmitted power
  - G_T = Transmitter antenna gain
  - G_R = Receiver antenna gain
  - λ = Wavelength

Path loss (or path attenuation) is the reduction in power density (attenuation) of an electromagnetic wave as it propagates through space. Path loss is a major component in the analysis and design of the link budget of a telecommunication system.

Shadow Fading

- Large-scale fading or Shadow fading
  - Slow spatial rate compared to wavelength
  - Slow rate of change
- Small-scale fading
  - Spatial dimension comparable to wavelength
  - Rapid rate of change

Fixed Wireless Network

- Fixed wireless access
  - a.k.a wireless local loop
- Point-to-multipoint network architecture
- **Benefits:**
  - Less capital investment
  - Quick and cheap to install and operate

MMDS Network (Multichannel Multipoint Distribution Service**)**

- Point-to-multipoint architecture
- Range between BSs is 50 km
- Operates over 2.5 to 2.686 GHz band
- Could operate on multichannel and hence capable of providing 2-way high- speed communication
- An implementation using cable modem equipment at both ends

LMDS (Local Multipoint distribution service)

- Point-to-multipoint architecture
- Covers 5 km radius; BSUs spaced 10 km apart
- Operates over 27-28.35 and 31-31.3 GHz bands
- Sensitive to rain attenuation
- Deploys cable modem equipment at both ends

MMDS / LMDS Network Management

- Head end:
  - Signals from multiple sources multiplexed
  - Frequency conversion for local signal
- NIU demarcation point between customer and service provider networks
- Cable modem: RF-to-Ethernet conversion

MMDS and LMDS will in the future migrate to 802.16 or WiMax standard.

- Subscriber station a more complex modem than CM (Cable Modem)
- **TDMA** (Time Division Multiple Access) downstream transmission
- **DAMA** (Demand Assigned Multiple Access) – TDMA upstream transmission

IEEE 802.16 Extensions (مهم)

- IEEE 802.16a: 2 to 11 GHz; Supports mesh deployment
- IEEE 802.16b: 5 TO 6 GHz; Real-time DiffServ service
- IEEE 802.16c: 10 to 66 GHz
- IEEE 802.16d: Improvement over 802.16a
- IEEE 802.16e (future)
  - Standard networking between carrier base stations
  - High-speed handoff with moving vehicles

Differentiated services or DiffServ is a computer networking architecture that specifies a simple, scalable and coarse-grained mechanism for classifying and managing network traffic and providing Quality of Service (QoS) on modern IP networks.

handoff is ability for transference is a design matter in mobile cellular system design. (مهم)

802.16d: MAC Layer

- Two sublayers
  - Convergence-specific: transport-specific
  - Common: independent of transport mechanism

Fixed BWA (Broadband Wireless Access) Management

- Components to be managed:
  - CM/SS management
  - BS management
  - Wireless link management
  - RF spectrum management
- 802.16 Recommendation OSI standards
- FCAPS functions managed (FCAPS = Fault, configuration, administration, performance, security)

Class of Service and QoS

- Elastic:
  - Interactive bursts (Telnet)
  - Interactive bulk (FTP)
  - Asynchronous bulk (email)
- Real-time
  - Guaranteed service (audio and video conferencing)
  - Predictive service (video playback)

Mobile and Wireless

- Mobile Network
  - A network with ability to perform computing anytime/anywhere
  - May or may not use wireless transmission medium
  - Types of mobility
    - Cellular: Always-on
    - Nomadic: Session not active while in motion
- Wireless Network
  - A network with wireless interface to computing devices and/or wired network
  - Deployed for networking both fixed and mobile users
- Mobile and Wireless Broadband Network Management
  - Management of integrated wired/wireless and fixed/mobile broadband – voice, video, and data networks

Mobile vs. nomadic

- **Mobile:** activities not disrupted when point of attachment is changed
- **Nomadic:** not active in motion; a.k.a. Portable computing

Mobile IP is analogous to call forwarding, except the forwarding address is mobile

3G Management Issues (مهم)

- Hierarchical LAN
- Joint management with wired network
- Mobile computing unit
  - Hardware limitations
  - Software limitations
- Mobility management
- Location tracking
- Resource management
- Wireless QoS management
- Power management
- Security management

Mobility Management

- Mobile IP (using Mobile IP to identify connected mobile units MUs)
- Location tracking
  - Discovery of Foreign Agents by Mobile Units
  - Broadcasting/advertising to locate an MU
  - Solicitation by MU
- Handoff management
  - Packet control function (PCF) / Radio Network
  - Handoff of PCF to PCF within PDSN
  - Handoff of PCF between PDSNs

Packet Control Function This is an entity in a radio access network that controls the transmission of packets between the BS (Base Station) and the PDSN (Packet Data Serving Node).

The Packet Data Serving Node, or PDSN, is a component of a CDMA2000 mobile network. It acts as the connection point between the radio access and IP networks.

Mobile IP Functions - Roaming

- Mobile IP uses two addresses: a fixed home address and a care-of-address that changes the point of attachment (FA)
- Mobile IP functions consist in:
  - Discovery of foreign agent (FA) and care-of-address
  - Registration of current location with FA and home agent(HA)
  - Tunneling of packets to and from the HA to FA care-of- address as mobile node roams

Discovery and Registration

- Mobile node discovers foreign agent (FA) and its care-of-address by advertisements of FA
- Mobile node can also discover by its solicitation
- Mobile node registers FA with HA

Functional entities in SNMP Management of Mobile IP:

- Mobile Node functional entity: A host or router that changes point of attachment from one network or subnet to another
- Home Agent functional entity: A router on a mobile node's home network, which tunnels packets to and from the mobile node via foreign agent
- Foreign Agent functional entity: A router on a mobile node's visited network, which provides services to the mobile node

Resource Management

- Scheduling and call admission control
  - Reservation of guard channels for handoff - static
  - Dynamic control of call admission – complex to control multimedia service
  - Proposals for QoS-based handoffs
- Load balancing between access networks
- Power management

Security Management

- WAP (Wireless Application Protocol) Security
  - WAP Wireless transport layer security (WTLS)
    - Based on transport layer security (TLS) or secured sockets shell (SSL)
    - "Walled garden" "vertical" integrated approach
- 3G network security
  - 3GPP (Third Generation Partnership Project) and 3GPP2 plan for IP to wireless device
  - Open standard SNMP based

VSAT is a popular implementation of direct transmission to home (DTH) satellite access network.

VSAT Components

- ODU Outdoor unit
  - Power amplifier • Up-converter • Down-converter
- IDU Indoor unit
  - Modems • Frequency synthesizer • Encoder / decoder
- Proxy agent for management; Later models with SNMP agent

Chapter 15

A home network or home area network (HAN) is a type of local area network with the purpose to facilitate communication among digital devices present inside or within the close vicinity of a home.

Home Networks

- Three access networks and modems
  - DSL • HFC • Wireless
- Four type of distribution networks
  - IEEE 1394 also known as FireWire
  - USB
  - LAN
  - Wireless LAN (WiFi) based on IEEE 802.11

Home Networking Technologies (مهم)

- Middleware and higher layer protocol networks
  - HAVi (Home Audio-Video interoperability)
  - Jini (Java-based middleware/network)
  - UPnP (Universal Plug and Play)
  - OSGi (Open Service Gateway initiative)
- Lower Layer wired protocol based networks
  - IEEE 802.3 Ethernet
  - VHN (Versatile Home Network)
  - IEEE 1394 (FireWire)
  - Cable
  - HomePNA (Home Phoneline Network Alliance)
  - HomePlug (Power Line Communication, PLC)
- Wireless LANs (Local Area Networks)
  - IEEE 802.11 WLAN
  - HomeRF
- Wireless PANs (Personal Area Networks)
  - IEEE 802.15.1 Bluetooth
  - IEEE 802.15.3a UWB (Ultra Wideband)
  - IEEE 802.15.4 Low data rate PAN

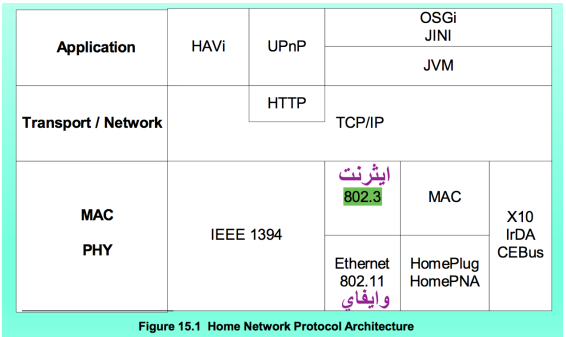


Figure 15.1 Home Network Protocol Architecture

Networking Protocols

Two Groups

- Physical interconnects
  - X-10
  - CEBus (Consumer Electronics Bus)
  - USB (Universal Serial Bus)
  - IrDA (Infrared Data Association)
  - HomePlug
  - HomePNA
  - WiFi 802.11
  - Bluetooth
  - Ethernet
  - IEEE 1394
- Service or application middleware
  - HAVi (Home Audio/Video interoperability)
  - UPnP (Universal Plug and Play)
  - Jini
  - OSGi (Open Services Gateway initiative)

HAVi Protocol Architecture (The HAVi device supports several types AV inputs **)**

Application for home entertainment and AV devices

- HAVi Components
  - Device
  - FAV (Full Audio Visual)
  - Intermediate AV (AV = Audio & Video)
  - Base AV
  - Legacy AV
- Device control module (DCM): Aggregate of FCMs
- Functional control module (FCM): Controls application functions
- Peer-to-peer environment

Jini Middleware

- Components
  - Device – Java object / Client
  - Access: RMI (Remote Method Invocation)
  - Services
    - Lookup
    - Discovery
- Based on Java platform
- Distributed environment for devices to communicate; Not housed in a single computer
- Forms impromptu communities – Group of shared service
  - impromptu = done without being planned, organized, or rehearsed.
- **Federation**: Jini communities linked together
- Jini surrogate host to handle non-Jini host
  - surrogate = a substitute بديل, especially a person deputizing for another in a specific role or office.
- JiniME (Mobile Edition) for mobile devices

UPnP Protocol Architecture (Universal plug and play**)**

- Active addition and deletion of devices
- Components
  - Devices
  - Services
  - Control points
- Peer-to-peer network

UPnP Network

- Underlying networks with standard protocols:
  - HomePlug
  - IEEE 1394
  - LAN
  - WLAN

OSGi Gateway (Open Service Gateway initiative**)**

- Platform for residential gateway
  - a **residential gateway** allows the connection of a local area network (LAN) to a wide area network (WAN). The WAN can be a larger computer network or the Internet.
- Specifies API only, not underlying implementation; Platform and application independent
- Service and device discovery functions
- Imports multiple discovery protocols and registers them as OSGi services
- Home Network Architecture
  - IEEE 1394 network for AV devices
  - IEEE 802.11 and Ethernet networks for mobile fixed data devices

Lower Layer Protocols for Networked Appliances

- Issues:
  - rt (REAL-TIME), near-rt (NEAR REAL-TIME), and non-rt, requirements
  - Multiplicity of component networks
  - Backbone QoS
    - A backbone is the part of the computer network infrastructure that interconnects different networks and provides a path for exchange of data between these different networks.
  - Interoperability

IEEE 1394

- Wired IEEE 1394
- Applicable to audio, video, and high-speed data

Category	Appliance	Protocol
Home Automation and Control	Lighting, Appliances, Climate Control	EIB, LonWorks, X10, CEBus
Entertainment	A/V Equipment, TV, PC	IEEE 1394
Communications	Telephone, Cell Phone, Intercom	IEEE 1394, HomePNA
Computers and Information	PC, Peripherals, PDA	Ethernet, WiFi

USB (Universal Serial Bus**)**

- Alternative to Ethernet as a computer peripheral interface
- Data-centric, not multimedia-oriented

USB 1.0	1.5 Mbps	Low speed	Cable length = 3m
USB 1.1	12 Mbps	Full Speed	Cable length = 3m
USB 2.0	400 Mbps	High speed	Cable length = 5m

802.11 PHY & MAC

- MAC Layer
  - CSMA/CA (CSMA/ Collision Avoidance) is used: (CSMA/CD in 802.3)
  - BSS Basic service set comprise AP (Access Point) and STAs (Stations);
  - Choice of coordination function by AP

DCF Distributed coordination function: is the fundamental MAC technique of the IEEE 802.11 based WLAN standard.

- Asynchronous
- Contention-based

PCF Point coordination function (optional): is a Media Access Control (MAC) technique used in IEEE 802.11 based WLANs.

- Synchronous
- Contention-free

- PHY Layer
  - 802.11b @ 2.4 GHz & data rate 11 Mbps
  - 802.11a @ 5 GHz & data rate 54 Mbps
  - 802.11g extends 802.11b to 54 Mbps with OFDM

802.3 is a standard specification for Ethernet, a method of physical communication in a local area network (LAN), which is maintained by the Institute of Electrical and Electronics Engineers (IEEE).

IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

Enterprise WLAN

- An access point (AP) and multiple stations (STAs)
- AP works as a bridge
- Every transmission is between AP and STA(s)

Security Management

Security for wireless LAN, WiFi , started with Wired Equivalent Privacy (WEP), which is a scheme trying to replicate the security in the wired network. Adding temporal key integrity protocol (TKIP).802.11i data protocols provide confidentiality, data origin authenticity, and replay protection. Authentication can be approved by either an EMP authenticator or by an external authenticator such as Remote Authentication Dial In User Service (RADIUS).

- WAP (Wireless Application Protocol) Security
- WAP Wireless transport layer security (WTLS)
- Based on transport layer security (TLS) or secured sockets shell (SSL)
- WEP (Wired Equivalent Privacy)
- WPA (WiFi Protected Access)
- WPA2 WPA with IEEE 802.11i
- 3G network security
  - 3GPP (Third Generation Partnership Project) and 3GPP2 plan for IP to wireless device
  - Open standard SNMP-based

WLAN Broadband QoS Issues

- Broadband comprises:
  - Voice: Real-time data
  - Video: Streaming data with/without delay
  - Data: Non-real time data
- Broadband QoS determined by MAC and PHY layers
- QoS Parameters:
  - Datarate
  - Delay bound
  - Jitter (slight irregular movement, variation, or unsteadiness, especially in an electrical signal or electronic device.)
- Two **sublayers** of media access (MAC)
  - DCF (Distributed Control Function): CSMA/CA
  - PCF (Point Control Function)
- Both DCF and PCF fail to satisfy broadband service
- Range dependencies
  - Power level
  - Antenna choice
    - Diversity antenna focuses beam
    - Diversity reception improves S/N ratio
    - MIMO (Multiple Input Multiple Output) technology enhances reception

WPANs (wireless personal area network**)**

is a low-range wireless network which covers an area of only a few dozen metres.

- 802.15.1 Bluetooth base line standard
- 802.15.2 Coexistence of 802 wireless technologies
- 802.15.3 High-rate radio (>20 Mbps)
- 802.15.4 Low-rate radio (<200 kbps)

Bluetooth Protocol Stack

- Short range up to 10m
- 2.042 GHz to 2.483 GHz band
- Time division multiplexing
- Voice support synchronous connection-oriented link
- Data support using asynchronous connectionless link

Chapter 16

Need for New Management Technologies

- Since late ’80s
  - Networks have evolved
  - Management needs have changed
  - Management technologies have evolved
- Mismatch in speed of evolution of networks and management requirements compared to the speed of management technology development

Evolution of Networks

- In the mid-late ’80s
  - Devices simple, resources constrained
  - Capabilities were limited
- Today
  - Increased functional complexity
  - Increased complexity in configuration
  - Increased intelligence and programmability of devices
  - Networks that provide a wide range of services
  - NGNs: Packet-based networks for all services
  - Providing unfettered (unrestricted) access for users to networks and to competing service providers for services of their choice

Next generation network (NGN) is a packet-based network that can be used for both telephony and data and that supports mobility.

Network Address Translation (NAT)

- NAT serves three main purposes:
  1. Provides a type of firewall by hiding internal IP addresses
  2. Enables a company to use more internal IP addresses. Since they're used internally only, there's no possibility of conflict with IP addresses used by other companies and organizations.
  3. Allows a company to combine multiple ISDN connections into a single Internet connection.

Changes in Operator Needs

- Management of large backbone networks requires powerful configuration management
- Move from device management approach to system management
- Service-centric view of network
- VoIP (residential and business), multimedia streaming, IP TV, fast data connectivity, triple play
- Increased speed of service delivery
- Automation of business processes

NGN Requirements (الجدول) →

Original Requirement	New Requirements
End-to-end transparency	Packet inspection, NAT
Peer-to-peer	NATs/firewalls/servers
Connectionless	MPLS
Best effort	Real-time demands, bandwidth demands
User back-off	QoS guarantees
Network empowerment	User empowerment
No flow state	Flow state
Trust	Hackers everywhere
Static addresses	DHCP, mobility
Fairness	QoS
Terminal-to-host	Mass public residential services, multiterminal, multi QoS
Flat network	Access and core domains
Simple protocol layering	Protocol maze
Research/Defense use	Commercialization, competition, consumer choice

Configuration Management Needs

- Need for concurrent configuration changes to several network devices
- Download bulk configuration changes on many devices
- Schedule configuration operations on devices at particular times
- Roll back support
- Coordinated activation of downloaded configurations

Roll back support= Return to a previously committed configuration.
The software saves the last 50 committed configurations, including the rollback number, date, time, and name of the user who issued the commit configuration command.

Datacomm is a privately held company, established in 1984

- SNMP based
- Aim was to have simple small footprint protocol
- Kept self contained and independent of other network services
- Catered to fault, performance monitoring, and simple configuration management
- Soon after release, shortcomings were exposed
- SNMPv2: Get-Bulk, Inform, SMIv2
- SNMPv3: security

○ Technology Solutions include:

- Network Security
- Network Management
- Messaging
- Consultation
- IPTelephony
- Cabling

Drawbacks of SNMP

- Inadequate information modeling – simple data structures and protocol operations
- Object based rather than object oriented
- No inheritance – so no information re-use
- Inadequate primitive for bulk information retrieval
- UDP transport restricts size of data sent
- Limited configuration management support
- Low level semantics

Overcoming SNMP Shortcomings

- Evolutionary efforts were made to address shortcomings
- Improving SMI
- Improving SNMP protocol
- Enhancing configuration management

The aim of the model is for Network and System Administrators to understand a number of issues and aspects. These include:

- Fault management and recovery
- Configuration and change management
- Accounting User Management
- Performance Management
- Security Management
- Application support
- Integration and Migration
- Planning for growth and acquisitions

Multi Technology Operations Systems Interface (MTOSI)
Standard that provides an integration framework for different applications in Service Provider's Operations Centre.

Organization for the Advancement of Structured Information Standards (OASIS) is a not-for-profit consortium that drives the development, convergence, and adoption of open standards for the global information society."

○ The two applicable standards are Management Using Web Services (MUWS) and Management Of Web Services (MOWS).

Management operations to monitor/control a Web service itself are specified. (MOWS)
Includes management-specific attributes to expose properties such as lifecycle state and performance of Web services.

تم بحمدلله ، بالتوفيق يارب .. ❤