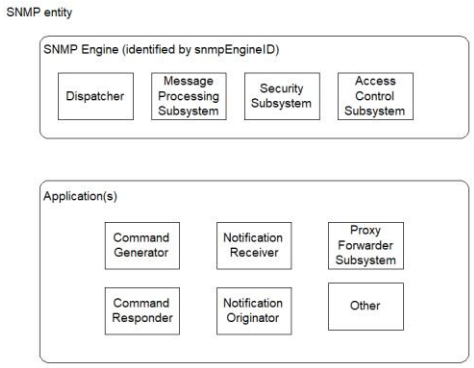
CH7

Key Features in SNMP V3

1. Modularization of document
2. Modularization of architecture
3. SNMP engine
4. Security feature
    - Secure information
    - Access control

SNMPv3 Architecture:



SNMP entity: is a node with an SNMP management element - either an agent or manager or both

Three names associated with an entity:

1. Entities: SNMP engine
2. Identities: Principal and security name
3. Management Information: Context engine

Dispatcher:

- One dispatcher in an SNMP engine
- Handles multiple version messages
- Interfaces with application modules, network, and message processing models

Dispatcher: Three components for three functions

1. **Transport mapper** delivers messages over the transport protocol
2. **Message Dispatcher** routes messages between network and appropriate module of Message Processor Subsystem (MPS)
3. **PDU dispatcher** handles messages between application and MPS (Message Processor Module)

Message Processing Subsystem:

- Contains one or more Message Processing Models
- One MPM for each SNMP version
- SNMP version identified in the header

Security

Security at the message level

- Authentication
- Privacy of message via secure communication

Access Control:

Flexible access control

- Who can access
- What can be accessed
- Flexible MIB views

Security Threats:

- **Modification of information:** Contents modified by unauthorized user, does not include address change
- **Masquerade:** change of originating address by unauthorized user
- **Fragments of message** altered by an unauthorized user to modify the meaning of the message
- Disclosure is eavesdropping
- Disclosure **does not require** interception of message
- Denial of service and traffic analysis are not considered as threats

Security Services:

1. Authentication
    - Data integrity:
    - Data origin authentication
2. Privacy / confidentiality: Encryption
3. Timeliness: Authoritative Engine ID, no. of engine boots and time in seconds

User-based Security Model:

- Based on traditional user name concept
- USM primitives across abstract service interfaces
    - Authentication service primitives
        - authenticateOutgoingMsg
        - authenticateIncomingMsg
    - Privacy Services
        - encryptData
        - decryptData

Privacy Module:

- Encryption and decryption of scoped PDU
- CBC - DES (Cipher Block Chaining - Data Encryption Standard)
- Encryption key
- Privacy parameter is *salt* value (unique for

Authentication Key:

- Secret key for authentication
- Derived from user (NMS) ID and password
- MD5 or SHA-1 algorithm based on implementation
- Authentication key is *digest2*

Authentication Parameters:

- Authentication parameter is Hashed Message Access Code (HMAC)
- HMAC is 96-bit long (12 octets)
- Derived from authentication key (*authKey*)

Access Control:

- View-based Access Control Model
    - Groups: Name of the group comprising security model and security name:
      In SNMPv1, is community name
    - Security Level
        - no authentication - no privacy
        - authentication - no privacy
        - authentication - privacy
    - Contexts: Names of the context
    - MIB Views and View Families
        - MIB view is a combination of view subtrees
    - Access Policy
        - read-view
        - write-view
        - notify-view
        - not-accessible

CH8:

RMON Components:

- RMON Probe
    - Data gatherer - a physical device
- Data analyzer
    - Processor that analyzes data

RMON: Remote Network Monitoring

RMON Benefits:

- Monitors and analyzes locally and relays data;
- Less load on the network
- Needs no direct visibility by NMS
- More reliable information
- Permits monitoring on a more frequent basis and hence faster fault diagnosis
- Increases productivity for administrators

RMON MIB:

- RMON1: Ethernet RMON groups (rmon 1 - rmon 9)
- RMON1: Extension: Token ring extension (rmon 10)
- RMON2: Higher layers (3-7) groups (rmon 11 - rmon 20)

RMON Groups and Functions:

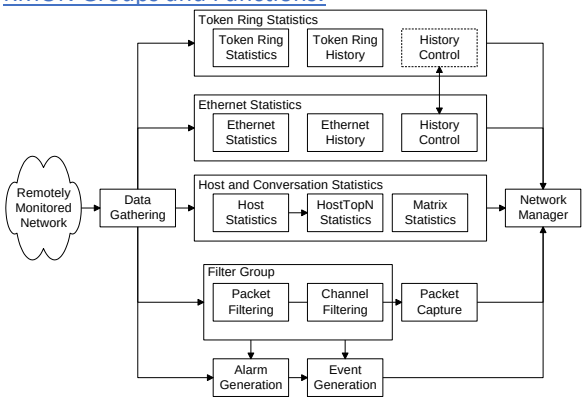


Figure 8.3 RMON1 Groups and Functions

RMON Functions:

- Statistics on Ethernet, token ring, and hosts / conversations
- The filter group is a cascade of two filters. The packet filter which filters incoming packets by performing a Boolean and/or XOR with a mask specified.
- The filtered outputs may generate either alarms or events. These are reported to the network manager.
- The output of the filter group could be stored in the packet capture module for further analysis by the network manager.

CH9:

Basic Network Software Tools: available as Part of the Operating System, Add-on applications.

- Status monitoring tools
- Traffic monitoring tools
- Route monitoring tools

Status Monitoring Tools:

NAME	OS	DESCRIPTION
Ifconfig	UNIX	Obtains and configures networking interface parameters and status
ping	UNIX Windows	Checks the status of node / host
nslook-up	UNIX Windows	Looks up DNS for name-IP address translation
dig	UNIX	Queries DNS server
host	UNIX	Displays information on Internet hosts / domains

ifConfig: Used to assign/read an address to/of an interface
Ping: Most basic tool for internet management, Useful for measuring connectivity and packet loss.
Nslookup: Converts a hostname into an IP address and vice versa querying DNS. Useful to identify the subnet a host or node belongs to.
Domain Name Groper(dig): Used to gather lots of information on hosts from DNS
Host: Displays host names using DNS
Traffic Monitoring Tools:

Name	Operating System	Description
ping	UNIX / Windows	Used for measuring roundtrip packet loss
bing	UNIX	Measures point-to-point bandwidth of a link
tcpdump	UNIX	Dumps traffic on a network
getethers	UNIX	Acquires all host addresses of an Ethernet LAN segment
iptrace	UNIX	Measures performance of gateways
ethereal, wireshark	Linux / Windows	Graphical tool to capture, inspect , and to save Ethernet packets

ping and bing: used to measure the propagation characteristics of the transmission path
ethereal and tcpdump: puts the network interface in promiscuous mode and logs the data.
Iptrace: uses NETMON program in UNIX and produces 3 types of outputs:

- IP traffic
- Host traffic matrix
- Abbreviated sampling of pre-defined number of packets

Packet Loss Measurement: Command: ping, Implementation varies from system to system
Snoop: Puts a network interface in promiscuous mode
Network Routing Tools:

Name	Operating System	Description
netstat	UNIX	Displays the contents of various network-related data structures
arp rarp	UNIX, Windows 9x/00/NT	Displays and modifies the Internet-to-Ethernet address translation tables
traceroute tracert	UNIX Windows	Traces route to a destination with routing delays

Route Tracing(traceroute): Useful for diagnosing route failures and detecting bottleneck nodes
Protocol Analyzer: Analyzes data packets on any transmission line including LAN, Measurements made locally or remotely
RMON Probe: Network Associates Sniffer, Used for gathering traffic statistics (instead of raw data) and used for configuration management for performance tuning.
Network Statistics:

- Protocol Analyzers
- RMON Probe / Protocol analyzer
- MRTG (Multi router traffic grouper)
- Home-grown program using *tcpdump*

MRTG: Multi Router Traffic Grouper

CH11:

Management Applications categories:

- Configuration management
- Performance management
- Fault management
- Security management
- Accounting management and reporting

Management Applications Reports:

- Service Level Management (SLA – Service Level Agreements)
- Policy-based management

Configuration Management:

- Network Provisioning
- Inventory Management
- Network Topology
- Database Considerations

Network Topology: Network topology should be updated for proper network management (Manual or Autodiscovery).

Fault Management: Fault is a failure of a network component, Results in loss of connectivity,involves 5 steps:

1. Fault detection:
    - Polling – manager polling agents for status- using ping for example.
    - generation of Traps: *linkDown, egpNeighborLoss – adv: faster failure detection, less traffic load.*
2. Fault location
    - Detect all components failed and trace down the tree topology to the source.
    - Fault isolation by network and SNMP tools- eg: use ping for packet loss, or snmp mib values like iferrors, ifdiscards etc.
    - Use artificial intelligence / correlation techniques
3. Restoration of service
4. Identification of root cause of the problem
5. Problem resolution

Performance Management: Data monitoring, problem isolation, performance tuning, analysis of statistical data.

- Tools: Protocol analyzers, RMON, MRTG
- Performance Metrics
    - Macro-level: Throughput, Response time, Availability, Reliability
    - Micro-level: Bandwidth, Utilization, Error rate, Peak load, Average load
- Data monitoring: Normal behavior, Abnormal behavior, Set up traps, Set up alarms for criticality
    - Manual (by an operator) and automatic (when the alarm condition clears) clearing of alarms.
- Problem isolation:
    - Manual mode using network and SNMP tools
    - Problems in multiple components need tracking down the topology
    - Automated mode using correlation technology
- Performance Statistics:
    - Traffic statistics
    - Error statistics
    - performance statistics are used in
        - QoS tracking
        - Performance tuning
        - Validation of SLA
        - Trend analysis
        - Facility planning
        - Functional accounting

Event Correlation Techniques:

- Rule-based reasoning
- Model-based reasoning
- Case-based reasoning
- Codebook correlation model
- State transition graph model
- Finite state machine model

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

Codebook phases:

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.

Codebook Enhancements:

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

Security Management:

- Security threats
- Policies and Procedures
- Resources to prevent security breaches
- Firewalls
- Cryptography
- Authentication and Authorization
- Client/Server authentication system
- Message transfer security
- Network protection security

Security Threats: SNMPv3 addressed security threats using USM (user-based security model) USM has two modules:

- Authentication module: Data integrity, Data origin,
- Privacy module: Data confidentiality, Message timeliness, Message protection

Policies and Procedures: Basic guidelines to set up policies and procedures:

- Identify what you are trying to protect.
- Determine what you are trying to protect it from.
- Determine how likely the threats are.
- Implement measures, which will protect your assets in a cost-effective manner.
- Review the process continuously and make improvements to each item if a weakness is found

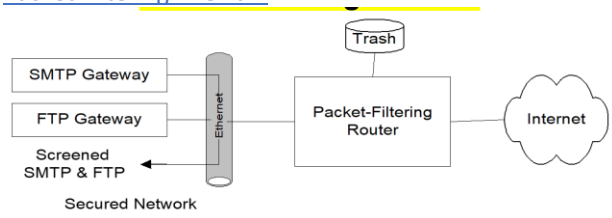
Firewalls: Protects a network from external attacks, Controls traffic in and out of a secured network, Could be implemented in a router, gateway, or a special host

Firewalls Benefits:

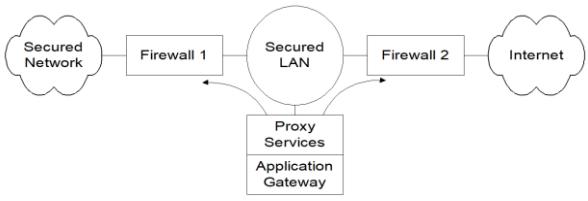
- Reduces risks of access to hosts
- Controlled access
- Eliminates annoyance to the users
- Protects privacy (e.g., finger)
- Hierarchical implementation of policy and and technology (e.g., finger)

Firewall types: Firewalls use packet filtering or application-level gateways

Packet Filtering Firewall:



Application Level Gateway:



Cryptography:

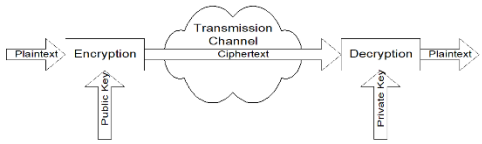
- Secure communication requires
    - Integrity protection: ensuring that the message is not tampered with
    - Authentication validation: ensures the originator identification
- Security threats
    - Modification of information
    - Masquerade
    - Message stream modification
    - Disclosure
-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

Secret Key Cryptography:

- Caesar cipher: each letter replaced by another letter, which is three (e.g. key of 3) letters behind in the alphabet
- Monoalphabetic cipher: Replace a letter with another randomly chosen; Maximum attempts to decode 26!

Public Key Cryptography:

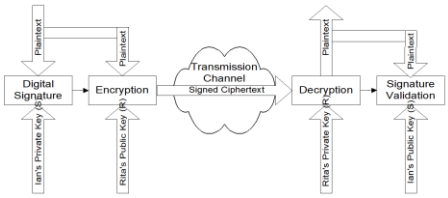
- Asymmetric cryptography - public and private key
    - Public key is distributed by the receiver to the senders to encrypt the message.
    - Private key is used by receiver to decode ciphertext Mailbox analogy
- Commonly used public key is RSA (Rivest, Shamir,and Adleman); 512-bit key, variable block size



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 Message Digest
- 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 2^{64} 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

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

CH12

Broadband Services:

- Broadband Integrated Services Digital Network (BISDN)
  - Voice, video, and data services
  - Transport protocol and medium – over the same medium
  - Very high data rate
- (Basic) Integrated Services Digital Network (ISDN)
  - 2B + D
  - Carries two 56 kilobaud (kbit) rate channels
  - One 8-kilobaud rate for signalization
  - Low-bandwidth network
- WAN: serves transportation over long distance between switching offices
  - Asynchronous Transfer Mode (ATM) Cell-based Technology –hybrid packet and circuit switched
  - Synchronous Optical Networks (SONET) / Optical carrier OC-n (n x 51.84 Mbps)
  - Synchronous Digital Hierarchy (SDH) / Synchronous Transport Signal (STS), MPLS
- LAN: cover last miles from the switching office to the customer premises equipment (CPE)
  - ATM LAN Emulation
- Access Technology
  - Cable modem / HFC – hybrid fiber coax
  - DSL
  - Wireless – terrestrial or satellite
  - Mobile wireless – GSM /GPRS , CDMA , WIFI

ATM Technology: five important concepts:

1. Virtual Path (VP) / Virtual Circuit (VC)
2. Fixed packet size or cell
3. Small packet size (53 bytes)
4. Statistical multiplexing-based on the speed of the devices, number of slots will be allotted.
5. Integrated services

Difference between ATM and Ethernet

- ATM is connection-oriented
- ATM makes one-to-one connection
- ATM 20-byte addressing scheme – dependent on topology

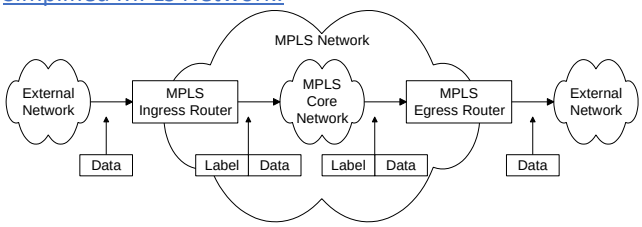
ATM WAN Reference Model:

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

OSI has defined five management interfaces:

- M1 Interface between private NMS and end user
- M2 Interface between private NMS and network
- M3 Interface between private NMS and public NMS
- M4 Interface between public NMS and network
- M5 Interface between public NMSs

Simplified MPLS Network:



- MPLS … Multiprotocol Label Switching combines IP and ATM
  - Richness of IP
  - Performance of ATM
- Forward Equivalent Classes (FEC) assigned at the ingress router and encoded in the label
  - FEC describes a set of packets with similar and / or identical characteristics which may be forwarded the same way
- Label is removed at the egress router and original protocol packet is sent out

Traffic Engineering (TE): Optimization of performance, for example avoiding over-utilized resources, etc. TE Topology updated whenever changes occurs in the network. RSVP (Reservation Protocol) – sets up route

(LSR): MPLS router called Label Switching Router

(LSP): End-to-end MPLS path called Label Switching Path

MPLS Label:

- MPLS Label is Short and fixed length – 32 bits – 4 octets, FEC locally significant identifier
- Label assigned by the downstream router
- Label is "shimmed" between layers 2 and 3 head

Label (20)	Exp (3)	S (1)	TTL (8)

Detection of LSP fault using 2 methods.

1. connectivity verification (CV) –specified by ITU-T
2. Bidirectional forwarding detection (BFD) – specified by IETF

LSP Fault scenarios:

1. Simple loss of connection
2. Misconnection
3. Swapped connection
4. Mismerging
5. Loop/unintended replication

LSP Ping: Modified Internet ping – is a UDP packet

Byte 1	Byte 2	Byte 3	Byte 4
Version Number = 1		Global Flags	
Message Type	Reply Mode	Return Code	Return Subcode
Sender's Handle			
Sequence Number			
TimeStamp Sent (seconds)			
TimeStamp Sent (microseconds)			
TimeStamp Received (seconds)			
TimeStamp Received (microseconds)			
TLV (Type Length Value)			

LSP Traceroute:

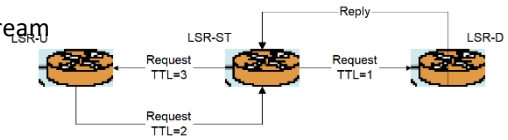
- Similar to IP traceroute
- Hop-by-hop fault localization as well as path tracing
- Packet sent to control plane of each transit LSR
- Transit LSR validates LSP
- Validates control plane against data plane of the LSR

Bidirectional forwarding failure detection (BFD):

- Uses LSP-ping MPLS 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
- Fast and low overhead detection between adjacent NEs
- LSP traceroute used for data path check in alternate paths

LSP Self-Test:

- Used for fault localization of an LSP
- Uses 3 LSRs, ST (self test), LSR-U upstream, and LSR-D downstream
- LSR-ST sends special LSP-ping to LSR-U with TTL=3
- LSR-U forwards it via LSR-ST to LSR-D with TTL=2
- LSR-D sends reply to LSR-ST completing the test
- Fault localized for link and node failures and notification sent out



MPLS Service Level Management:

- SLA between Service Provider and customer
- SLA management involves fault and performance management
- Multiple protection paths (if fault between R3 and R4)
- LSP1 PROTECTION global protection
- Nested path LSP 2 local protection path

CH13

Cable Access Network:

- Head end:
  - Signals from multiple sources multiplexed
  - Frequency conversion for local signal
  -
- Traffic Flow: a pair of optical fibers
  - Downstream (forward path signal): Head end to NIU
  - Upstream (reverse path signal): NIU to head end
- Network interface device(NID)/unit(NIU): Demarcation point between customer network and service provider networks
- Cable modem: RF, Ethernet, voice-over-IP and video

Cable Access Network Technology Transmission Mode:

- Downstream: Time Division Multiplexing (TDM) broadcast mode
- Upstream: Time Division Multiple Access (TDMA) / Synchronous Code Division Multiple Access (S- CDMA)

Cable Access Network Technology:

- 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 It allows several users to share the same frequency channel by dividing the signal into different time slots
- Code-division multiple access (CDMA) is a channel access method used by various radio communication technologies

Modulation Schemes:

- 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)

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.

Shannon limit of data rate is 30,000 bps

DSL Limitations:

- Loop conditions with no direct copper to the house
- Loaded coils in loop (used to increase analog distance) cannot carry digital signal
- Modern subdivisions have fiber to the neighborhood or curb (end near homes) with digital mux (multiplexer)
- Operating company inventory dated (administrative issue)

xDSL 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
SHDSL	Symmetric High data rate DSL	5.6 Mbps	Duplex Duplex	2-pair	Business Connections
VDSL 1 Km	Very high data rate Digital Subscriber Line	55 Mbps 15 Mbps	Down Up	2-pair	Triple Play (No QoS)
VDSL2- Long Reach 3 Km	Very high data rate Digital Subscriber Line	55 Mbps 30 Mbps	Down Up	2-pair	Triple Play
VDSL Short Reach 500 m	Very high data rate Digital Subscriber Line	100 Mbps 100 Mbps	Down Up	2-pair	Triple Play

Splitter separates voice and data

Modulation Schemes:

- Carrierless amplitude phase (CAP) modulation
- Discrete MultiTone modulation (DMT): 4kHz tones
- Both CAP and DMT are QAM-based

VDSL Network:

- Used in FTTN configuration
- Asymmetric band allocation (similar to ADSL)
- Fiber carries multiple channels to ONU
- Channels demultiplexed at Optical Network Unit (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

Interfaces: An interface can have multiple physical connections

- V interface V_C interface between access node and external network and interfaces
- U interfaces - off the splitters
- POTS interfaces – low-pass filter interfaces for POTS

ADSL Channeling Schemes:

- Transport bearer channels
- Buffering scheme
  - Fast channel: uses fast buffers for real-time data
  - Interleaved channel: used for non-real-time data (digital data channel)
  - Both fast and interleaved channels carried on the same physical channel

ADSL Network Management Elements:

- Management communications protocol across V-interface
- Management communications protocol across U-interfaces
- Parameters and operations across ATU-C
- Parameters and operations across ATU-R
- ATU-R side of the T interface

Management of physical layer involves:

- Physical channel
- Fast channel for RT
- Interleaved channel for NRT

Performance Management Parameters:

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

ADSL Profiles Management:

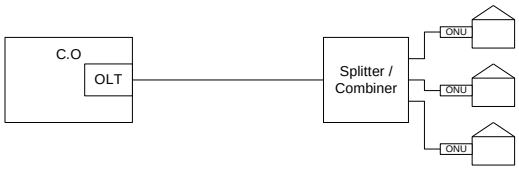
- Configuration profile
- Performance profile
- Alarm profile
- Traps (Generic, Loss of frame , Loss of signal , Loss of power, Error-second threshold , Data rate
- change, Loss of link ,ATU-C initialization failure)

Configuration Profile Mode: Dynamic, Static

Passive Optical Network:

- Fiber Medium: Can be implemented on copper
- No active elements (regenerative repeaters, amplifiers, …) in the transmission medium
- Passive elements in the fiber medium: Beam splitter – Lossy

PON Configuration: EPON (Ethernet PON):



CH14

Wireless Broadband Networks:

- Access Networks: MAN authentication Key Agreement. WiMax
- 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 (signal strength degrades): short and long
- Doppler effect (when the source or receiver moves fast with respect to each other

Shadow Fading:

- Large-scale fading is also called Shadow fading
  - is the result of signal attenuation due to signal propagation over large distances
  - Slow spatial rate compared to wavelength
  - Slow rate of change
- Small-scale fading
  - Spatial dimension comparable to wavelength
  - Rapid rate of change

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

3G Management Issues:

- 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

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 uses two addresses:

- a fixed home address
- care-of-address that changes the point of attachment

Mobile IP functions:

- Mobile Agent (Mobile Node) Discovery of foreign agent (FA)
- 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 SNMP Management of Mobile IP:

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

QoS Management:

- QoS support for last leg between access point and mobile node
- Depends on mobility and resource management
- 3GPP/3GPP2 (3G Partnership Project) standards ensure interoperability
- 3GPP has defined four QoS classes (TS 23.107) shown above
- Telephony handled using SIP (session initiation protocol)
- Backbone based on DiffServ

Very Small Aperture Terminal (VSAT): is a popular implementation of direct tx to home (DTH) satellite access network. Used for back-up link + in rural areas

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