Access Networks and the Local Loop

(la boucle locale)
The Local Loop solutions

- WiMAX
- Mobile 3G
- Mobile 4G
- ADSL
- Cable modem
- Optical fiber
Access Networks Evolution

- A large number of recent technologies:
  - xDSL and unbundling of the local loop
  - CATV, HFC (Hybrid Fiber Coax)
  - FTTx, PON
  - Power Line Communication (PLC)
  - WLL (Wireless Local Loop)
    - 802.11 (WiFi)
    - 802.16 (Wimax)
    - Satellites (LEO/MEO/GEO)
    - 3rd Generation Mobile Systems (UMTS)
    - LTE, femtocells
  - ...

Typical wired access infrastructure (2)

Typical infrastructure of incumbent telecom operators

WDM: Wavelength Division Multiplexing
SDH: Synchronous Digital Hierarchy; ATM: Asynchronous Transfer Mode
DSL: Digital Subscriber Line
Typical wired access infrastructure
Length of the Local Loop

France
Communication medium (wire)
xDSSL access evolution: ATM vs Ethernet
The Optical Loop

- FITL (Fiber In The Loop) or FTTX (Fiber To The X)
  - X=E, Exchange
  - X=C, Cabinet, Curb
  - X=B, Building
  - X=O, Office
  - X=H, Home

- FTTX development examples
  - FTTH by Free (FR), FTTB by Numericable (FR), Fastweb (IT)
  - Future: FTTE/FTTC + femtocells

- FTTX usually based nowadays on Ethernet MAN with
  - Direct fiber connections (mainly for SOHO and LA)
  - Use of Ethernet PONs
  - Use of remote DSLAMs (e.g. VDSL)
FTTH/B evolution
PON (Passive Optical Network)

OLT: Optical Line Terminaison   ONU : Optical Network Unit

APON
ATM PON
EPON
Ethernet PON
GPON
Gigabit PON

OLT: Optical Line Terminaison   ONU : Optical Network Unit
PON (Passive Optical network)

PON minimised the required switching equipment in the access
The Cable Loop (CATV)

- Reusing existing CATV equipment
  - Inexisting in some countries
  - Widely deployed in some others (North America)
  - Upload channel problem
CATV Access Network
The xDSL Loop
The ADSL modulation

20 canaux (4 kHz / canal)  
8 bits par intervalle d’horloge  
⇒ 20 × 4,000 × 8 = 640 kbit/s

256 canaux (4 kHz / canal)  
8 bits par intervalle d’horloge  
⇒ 256 × 4,000 × 8 = 8,2 Mbit/s
ADSL: bandwidth-distance constraints

Maximum capacity (in Mbit/s) vs Distance (in kilometers)

- PABX
- Data Network
- ADSL
ADSL evolutions

- ADSL 2
  - New coding and modulation techniques, leading to:
    - More bandwidth (maximum rate of 10Mbps downstream, approx 1Mbps upstream) at a given distance
    - Or longer reachable distances (for a given rate)
  - Inverse Mux, possibility to use lower frequencies

- ADSL 2+
  - Higher frequency range for download
  - Leading to a maximum of 25 Mbps for download (for VERY short distances)
  - Same frequency range for upload. Still 1Mbps.
The DSL wiring and unbundling

ULL: Unbundling Local Loop
(at the concentrator level or DSLAM level)
xDSL bandwidth-distance product

- ADSL (Asymmetric Digital Subscriber Line)
- SDSL (Symmetric DSL)
- HDSL (High-bit-rate DSL)
- VDSL (Very-high-bit-rate DSL)
xDSL spectral utilization

POTS
(plain old tel. service)

25 kHz
upstream
downstream

1,1Mhz
2,2Mhz

ADSL
ADSL2
ADSL2+

VDSL

12Mhz

10Khz 100Khz 1Mhz 10Mhz
DSL Triple play

IP – Ethernet (VLANs)
Wi-xx telephone

Téléphone Wi-Fi

Téléphone Wi-Fi/GSM/XX
The quadruple play

- Domicile
- Box- Modem DSL

- Wi-Fi visité
The Wire-Less Loop (WLL)

No real applications in early 2000s
Nowadays new products and protocols (4G, WiMax, LTE) → bypass DSL
The Wire-Less Loop (2)

- Cellular Network: up to 2Mbps (UMTS)
- IEEE 802.11 (WiFi)
  - 11Mbps (11.b), 54Mbps (11.a et 11.g), 100Mbps under investigation
  - Limited coverage
- WiMax (IEEE 802.16)
  - 802.16a (deployed early 2005):
    - Point to point connection up to 134Mbps.
    - Point-to-multipoint: up to 75Mbps for cells of several kms
    - Target: Fixed access
  - 802.16e:
    - Includes roaming (speed around 100km/h)
    - Target: mobile broadband access
- Long Term Evolution (LTE)
  - 326 Mbps dw, 86 Mbps up
  - To replace DSL, especially in fast developing regions
  - Higher penetration in rural areas than WiMax
The Satellite Loop

LEO (Low Earth Orbit)
500 – 1,500 km

MEO (Medium Earth Orbit)
5,000 – 12,000 km

GEO (Geostationary Earth Orbit)
36,000 km
Home network
Home network communications

- Transport
  - Ethernet
  - PLC (Power Line Communication)
  - Wireless
    - Wi-Fi

- Major standards
  - UPnP: Universal Plug&Play
  - DLNA: Digital Living Network Alliance
The Power Line Loop
Power Line Communication (PLC)
Remote Access
The legacy remote access architecture

Remote user

Remote access

Remote (or Network) Access Server
RAS (NAS)

Corporate Headquarters
or ISP PoP

Internet
Intranet
Need for new functions

- **At the user side**
  - Need for a Link Layer (LL) protocol to pass through the p2p line.
  - Encapsulation of different protocols
  - Security:
    - Encryption
  - Addressing issues (facilitate configuration)

- **At the other side (ISP or corporate network)**
  - Security
    - Authentication, Access control
  - Addressing issues (lack of IPv4 addresses)
  - Need for a centralized management
Need for new functions (2)

- Intelligence has to be added in the dial-in machine:
  - LL, Multiplexing
  - Should be able to reply to specific Authentication request from RAS.
  - May support encryption
  - Should support negotiation and control functions (get IP address, encryption used or not? etc.)

- RAS (or NAS, or BRAS)
  - LL, Demultiplexing
  - Should support specific protocols to authenticate dial-in user
  - Should be able to disable some packets based on Access Control Policies
  - May support encryption
  - Should support negotiation and control functions (see dial-in user)
  - Should be able to access specific information on the user (AAA)
  - May have a pool of IP Addresses for dynamic address assignment
Need for new protocols

• Dial-in user ↔ RAS

  The Point to Point Protocol (PPP)
  • HDLC-like encapsulation over any physical medium
  • Specific *negotiation and control* sub-protocols (LCP, NCP, ECP, CCP).
    - LCP allows negotiating the authentication scheme
    - NCP allows for IP address dynamic assignment
  • Specific *authentication* sub-protocols (PAP, CHAP, EAP, OTP)
  • Specific *compression and encryption* sub-protocols
  • Used over many networks; for xDSL, over Ethernet (PPPoE) or over ATM (PPPoA)

• RAS ↔ AAA Server
  • RADIUS: Remote Dial In User Service
  • TACACS: Terminal Access Controller Access Control System
The remote access legacy architecture

Remote user

Remote access

PPP

Remote (or Network) Access Server

AAA server

User profile database

Corporate Headquarters or ISP POP

Internet

Intranet
Point to Point Protocol (PPP)
PPP has 3 main components:

- A method for encapsulating multi-protocol datagrams
- A Link Control Protocol (LCP) for establishing, configuring, testing, maintaining, and finally terminating the data-link connection
- A family of Network Control Protocols (NCPs) for establishing, configuring, maintaining, and finally terminating different network layer protocols sessions

PPP includes many other components (optional):

- A family of Protocols for user Authentication (PAP, CHAP, EAP, ...)
- Protocol for Encryption Control (ECP)
- Protocol for Compression Control (CCP)...
- ...

PPP components
PPP encapsulation: HDLC-like framing

<table>
<thead>
<tr>
<th>F</th>
<th>A</th>
<th>C</th>
<th>P</th>
<th>INFO</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>Max 1500</td>
<td>2</td>
</tr>
</tbody>
</table>

- **F**: HDLC Flag coded 0111 1110
- **A**: Address coded 1111 1111 (All-Stations address)
- **C**: Control coded 0000 0011 (Unnumbered Information with P/F=0)
- **P**: Protocol coded to indicate the network layer protocol used or eventually, an LCP, authentication or other control packet
- **INFO**: Information field (default: 1500 octets long maximum). May include padding.
- **FCS**: Frame Check Sequence 16-bits long default, may be 32-bits long.

HDLC: High-level Data Link Control
Exemple: PPP over ATM with xDSL
PPP link life cycle

- Link dead
- Link establishment
- Authentication
- Network Layer Protocol exchange
- Link Termination

States:
- UP
- OPENED
- FAIL
- SUCCESS/
  NONE
- CLOSING
- DOWN

Transitions:
- UP to OPENED: SUCCESS/
  NONE
- OPENED to FAIL: FAIL
- FAIL to DOWN: FAIL
- DOWN to UP: UP
- OPENED to CLOSING: CLOSING
The role of LCP and NCP

- LCP main goals:
  - Negotiation of link parameters, like maximum frame size
  - Negotiation of authentication method

- NCP:
  - Each network protocol has its proper NCP
  - The NCP for IP is called IPCP (IP Control Protocol)
    - dynamic allocation of an IP address for the remote host
    - Negotiation of compression method
PPP Authentication protocols

- The authentication protocol to be used is **negotiated** through LCP during the link establishment phase.
- Then, the **authentication phase** takes place as soon as the link is established.
- Possible Authentication Protocol:
  - PAP: Password Authentication Protocol (legacy clear text password exchange...no longer used)
  - CHAP: Challenge Handshake Authentication Protocol
  - EAP: Extensible Authentication Protocol
  - ...
Example configuration (PPP over PSTN)
Example configuration

Protocols multiplexed on top of PPP (IP only in this example for security reasons...)

RAS server access via PPP
Example configuration (continued)

Authentication Protocols allowed at PPP session set-up

- Utiliser le protocole EAP (Extensible Authentication Protocol)
- Protocole SPAP (Shiva Password Authentication Protocol)
- Protocole CHAP (Challenge Handshake Authentication Protocol)
- Protocole Microsoft CHAP (MS-CHAP)
- Protocole Microsoft CHAP Version 2 (MS-CHAPv2)
AAA server
AAA servers (1)

Remote user

Remote access

Corporate network or ISP network

User profile database

RAS/NAS

AAA server

RADIUS

AAA servers (2)

- AAA servers are responsible for the
  - **Authentication (centralized)**
  - **Authorization (access control)**
  - **Accounting (facturation)**

for the entire set of RAS deployed as gateways to the corporate or ISP network.

- AAA servers are connected to **user profile databases** where the information relative to each user is maintained
  - Authentication procedure
    - Password, secret...
  - Services **authorized**
    - Information relative to the service, and to particular services...
  - **Billing information**
AAA servers (3)

- When a user tries to access the network via a RAS
  - the **RAS interrogates the AAA server** in order to
    - Authenticate the user
    - Know what services are to be offered to this user
    - Know what are the particular options with which these services should be offered
  - The RAS asks the AAA server to **do the accounting for the connection**
    - This could have been done by the RAS itself. However, since many RASs may be deployed for a given network (typical case for ISPs), a centralized AAA server/user database is advisable
RADIUS

- RADIUS (Remote Authentication Dial-In User Service)
  - standardized protocol
    - RFC 2138, 2139 for the accounting part
  - describes the communication between a RAS (the Client) and an AAA server called the RADIUS server
  - communication protected by authentication and encryption

- The RADIUS protocol is a flexible protocol allowing to support
  - Multiple authentication mechanisms (PAP, CHAP, EAP...)
  - Extensions to cope with new architectures such as IPsec, tunneling, dial-in roaming...
- RADIUS packets are transmitted over a UDP/IP stack
RADIUS with CHAP authentication

Authenticating Peer  RAS  RADIUS Server

LCP Configure-Req     LCP Configure-Ack
(CHAP Auth)            

CHAP Challenge        CHAP Challenge
(Challenge Value)      

Radius Access-Req     Radius Access-Accept
(UserName             (Config Info)
ChapChallenge
ChapPassword=Chap Id +
Response Value (encrypted)
RAS Id
RAS Port)             

CHAP Auth complete    CHAP Success
NCP phase starts
Virtual Access Network
Tunnelling
Traditional dial-in user service
Direct corporate access

Multiple protocols may be supported by the PPP connection
Private RAS-managed IP addresses may be used in the IP packets

BUT the call may be long distance!
Traditional dial-in user service via-ISP access

Only IP packets may traverse the Internet domain
Only public IP addresses may be used in the IP packets
Virtual Dial-in user service

PPP header
PPP | Orig IP hdr | TCP/UDP | Data

PPP + IP tunneling
New IP hdr | PPP encapsulating header | PPP | Orig IP hdr | TCP/UDP | Data

Dial-in user
LOCAL CALL

AC : Access Concentrator
NS : Network Server

Corporate network