**COMP312-09A
Communications and Systems
Software**

Access Protocols PPP vs. DHCP
Richard Nelson
richardn@cs.waikato.ac.nz

Overview

- The problem
- PPP
- DHCP
- User identities
- Assignment of IP addresses
- Assignment of other parameters
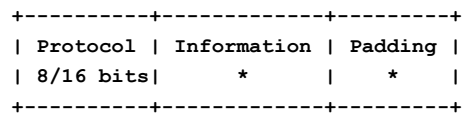

DSL connection

The Problem
- The Network has to talk to the customer router
  - To assign addresses (gateway, DNS)
  - To allow user login
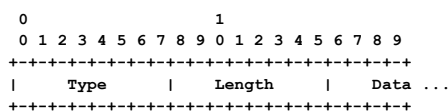- On serial lines packets had to be encapsulated somehow.

PPP

- Point-to-Point Protocol (RFC 1661)
  - A method for encapsulating multi-protocol diagrams
    - Layer 2 in OSI stack
  - A Link Control Protocol (LCP) for establishing, configuring, and testing the data-link connection
  - A family of Network Control Protocols (NCPs) for establishing and configuring different network-layer protocols
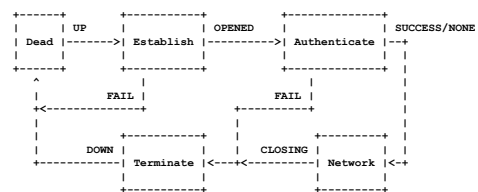
PPP Encapsulation

```
+----------+-------------+---------+
| Protocol | Information | Padding |
| 8/16 bits|      *      |    *    |
+----------+-------------+---------+
```

The least significant bit of the most significant octet must be zero

PPP LCP

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |    Length     |  Data ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Identify Maximum receive unit (MRU)
- Echo-request/echo-reply
- etc

PPP

```
+------+      +-----------+        +--------------+
|      | UP   |           | OPENED |              | SUCCESS/NONE
| Dead |----->| Establish |------->| Authenticate |--+
|      |      |           |        |              |  |
+------+      +-----------+        +--------------+  |
   ^             FAIL |              FAIL |          |
   +------------------+     +------------------+     |
   |                  |     |                  |     |
   |          DOWN    +-----------+   CLOSING   +---------+   |
   +-----------|Terminate |<---+<----------| Network |<-+
              +-----------+                +---------+
```

RFC 1661, Page 6

PPP NCP for IP

- IP Control Protocol (RFC 1332)
- Used to set IP addresses
- IP compression method (if desired)
  - VJ TCP/IP compression – RFC 1144

PPP NCPs

- Other NCPs
  - IPv6
  - Appletalk
  - IPX
- Multiple protocols can co-exist on a PPP link

PPP

- Used extensively in dial-up ISP environments
  - Convenient method of user authentication
  - PAP: Password Authentication Protocol
  - CHAP: Challenge-handshake Authentication Protocol
- Also in many DSL environments
  - PPP infrastructure in place, so just reuse it for different access technology
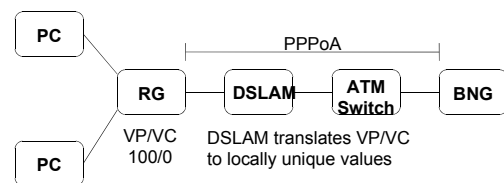
PPPoA

Figure 5.1

PPPoA

- Point-to-Point
  - Residential Gateway (RG) peers directly with BNG
- Using circuit switched network
- PPP frame encapsulated in ATM AAL5 frame.
- RFC2364
- Large MTU

PPPoE

- Ethernet: shared access medium
- PPPoE: point-to-point connection transported over Ethernet
  - Often over ATM to DSLAM
  - Possibly Ethernet over ATM to BNG
- RFC 2516
- MTU lower than standard Ethernet due to PPP framing
- Can used mixed Ethernet and ATM networks

PPPoE

- Since Ethernet is inherently multipoint, PPPoE includes a discovery phase.
- Allows possibility of choosing the other endpoint.
- Allows multiple point-to-point connections to exist to different BNGs from one RG
- Bridged RG
  - RG passes PPPoE frames from ADSL to Ethernet for another device to terminate PPPoE link
- Routed RG
  - RG terminates PPPoE and routes packets to Ethernet (Usually with NAT)

Advantages of PPP

- Strong, flexible and extensible Authentication
- Per session state information - "keepalives"
- Easy identification of user sessions
  - Billing
  - QoS
  - Lawful Intercept
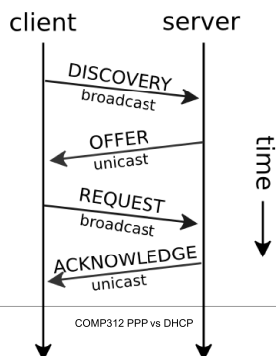- Multiprotocol support
- Well understood

But

- In modern networks DSLAMs are IP/Ethernet connected
- So if you have Ethernet from the DSLAM to the BNG why do you need PPP Framing?
- Why not use a protocol with no framing that is designed for device configurations
- Dynamic Host Configuration Protocol

DHCP

- Dynamic Host Configuration Protocol
  - RFC 2131
- Application-layer protocol
- Designed for broadcast networks
- UDP broadcast from port 68 to port 67

- DHCP
  - Assign IP addresses, DNS servers, etc.
  - Configure SIP handsets, set top boxes
  - No authentication

DHCP Process

client   server

DISCOVERY
broadcast →

← OFFER
unicast

REQUEST
broadcast →

← ACKNOWLEDGE
unicast

time →

DHCP Phases

- Discovery
  - Broadcasts to find servers. Routers will only forward these if specifically configured to.
- Offer
  - DHCP Server(s) provide IP address, Mask, Lease duration and other details based on configured information
- Request
  - Client chooses from the offers received. Other servers see the request and withdraw their offers. May include request for further configuration.
- Acknowledge
  - Server acknowledges the request and includes extra configuration if required and available.

Allocation

- Configuration Information (mainly IP address) can be assigned three ways.
- Dynamically. Next free address is allocated from a pool (or pools). Addresses are reallocated if leases expire without renewal.
- Automatic. Next free address allocated from a pool. Server remembers IP address for that client.
- Static. Server is configured with information to allocate specific addresses to specific clients based on hardware ID (normally MAC address).

DHCP Options

- RFC2132 is dedicated to options
- Options for
    - Servers: DNS, NTP, Logging etc
    - Network: Mask, MTU, ARP, routes etc
    - Per Interface options
    - Link Layer Parameters
    - TCP, Keepalive, TTL, etc
    - Application and Service Parameters
    - DHCP protocol options
- A process is provided for establishing new options
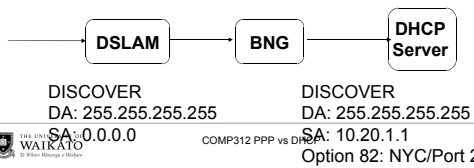
DHCP in ADSL Networks

- Addresses are leased --- defined by TTL
    - DHCP client renews its lease when it has reached half-way with its lease
- Numerous options to supply extra configuration
- No Keepalives
- No authentication capability
    - What about using the MAC address?
    - Other ways of identifying customer?

Keepalives

- Captive portals use open browser session
    - But what about SIP phone
- Can use
    - ARP
    - Ping
    - Bidirectional Forwarding Detection

DHCP Option 82

- Have DSLAM insert option identifying customer port
  - Transparent to customer
  - Therefore hard to forge
  - RFC3046
  - No Authentication of end user

```
          ┌────────┐      ┌──────┐      ┌─────────┐
─────────▶│ DSLAM  │─────▶│ BNG  │─────▶│  DHCP   │
          └────────┘      └──────┘      │ Server  │
                                        └─────────┘
```

DISCOVER
DA: 255.255.255.255
SA: 0.0.0.0

DISCOVER
DA: 255.255.255.255
SA: 10.20.1.1
Option 82: NYC/Port 20

DHCP Authentication Extensions

- New work in IETF
- Specifically intended for DSL Networks
- Supports Extensible Authentication Protocol
- Requires both RG and BNG support
- Supports both IPv4 and IPv6

DHCP models

- BNG-hosted DHCP
  - Local address pools
  - Limited control over address allocation policy
- DHCP relay
  - BNG relays DHCP to central server
  - BNG has no lease state
- DHCP relay proxy
  - BNG masquerades as DHCP server
  - More complex functionality required on BNG to add new DHCP option types

---

DHCP Summary

- Purpose designed configuration protocol for IP environment
- Session status provided via other means
- Authentication missing but solutions available as extensions
- No overhead in user data packets
- Supports redundant gateways

PPP vs DHCP

- Why are we interested in replacing PPP
- Need to run a full protocol state machine on a per-subscriber basis
  - Large processing overhead on an a expensive part of the infrastructure
- Not easy to provide complex configuration to RG for support of voice and video
- Overhead in every packet
  - Can cause MTU complications

PPP vs DHCP cont

- But DHCP has disadvantages too!
- No session state -use other mechanisms
- Limited authentication support – solution coming
- Further difficulties in wholesale environments but solutions available for that too.