The Evolution from PPPoE to IPoE sessions

Horia Miclea, hmiclea@cisco.com
Cisco Systems, Service Provider Systems Development
Agenda

- From PPP to IP, a natural evolution
- Carrier Ethernet Service Delivery Models
- Intelligent Service Gateway for PPPoE and IPoE
  - Overview
  - ISG IP Session Models
  - IP Sessions Additional Considerations
- Conclusion
PPP to IP, A Natural Evolution
For Carrier Ethernet Triple Play Services

- Broadband Access Technology options are evolving and diversifying while having two common technology denominators, Ethernet multiplexing/aggregation and IP services
  - WiMAX 802.16D/E gets traction in emerging worldwide markets
  - New DSL flavours (ADSL2+ and VDSL) defined an Ethernet baseline for the Access Nodes at the UNI and NNI level
  - Metro FTTX P2P (802.3ah) and MP (PON) deployments are increasing in relevance for both residential and business services

- Triple/Quad Play services like IPTV and VOD have imposed IPoEthernet as service encapsulation baseline
  - PPPoE may still be used for Internet Access

- High market penetration targets requires advanced subscriber management functions for PPPoE and IPoE service models to optimize the operational costs
  - And to enable mass customization of the broadband services

- Cisco offers “Intelligent Services Gateways” to address the PPPoE to IPoE migration while maintaining all subscriber management functions
Carrier Ethernet Architectures and Service Delivery Models
Carrier Ethernet Architecture Models

- **Operational & cost considerations drive two architectures models:**
  - Distributed and Centralised IP Edge Architectures

- **Drivers for the centralized edge architecture**
  - Align with existing SP organizational and operational structures
  - An order of magnitude fewer subscriber state aware network elements to manage
  - May improve the CAPEX efficiency especially if services planned allow network oversubscription
  - Operational and organizational differentiation into access, aggregation, edge and core network layers

- **Drivers for the distributed edge architecture**
  - Single point of implementing (L2/L3) services edge
  - Consolidation of functions eliminates differentiated infrastructure
  - Simplified operations by removing the overlay circuit based aggregation network transport
  - Increased penetration of 3play services (VOD) drives lower oversubscription on the aggregation network and makes less suitable centralized edge devices
  - Increased flexibility for local content injection, network based admission control for VoD and more optimal handling for peer to peer traffic

*Notes:*

An MPLS/IP transport for the Core & Aggregation layers can accommodate both architecture models

These two architecture models may be combined on a service basis in the scope a network deployment for meeting certain practical considerations (for example centralised edge for Internet Access while it already exists and distributed Video and Voice services edge to optimize the costs)
Centralised Services Architecture Options

HSI, VoIP, VoD
Non Trunk N:1 or 1:1 VLAN TV
N:1 VLAN

HSI/VoD/VoIP
IP Multicast or Multicast VPN

HSI, VoIP, VoD, TV
ISG Sessions

TV
SP Peering

HSI, VoIP
Trunk N:1 or 1:1 Service VLAN TV, VoD
N:1 VLAN

HSI/VoIP
VOD
IP Multicast or Multicast VPN

L2 IP/PPoE or Interface Sessions
ISG Sessions

VOD
TV

Efficient Access
Large Scale Equal Access Aggregation
Retail & Wholesale Intelligent Edge
Multiservice Core

Efficient Access
Large Scale Equal Access Aggregation
Retail & Wholesale Intelligent Edge
Multiservice Core

Access Node
Aggregation
Distribution
Core

MPLS L2/L3 services VPWS/H-VPLS/IP Multicast
BNG

MPLS
ISG

DSL, PON, Ethernet, WiMAX

© 2007 Cisco Systems, Inc. All rights reserved.
Distributed Services Architecture Options

- **HSI, VoIP, VoD, TV**
- **Non Trunk N:1 or 1:1 VLAN TV**
- **N:1 VLAN for 1:1 VLAN model**

- **HSI and/or VoIP**
- **Trunk N:1 or 1:1 Service VLAN TV, VoD**
- **Trunk N:1 or 1:1 Service VLAN TV**
- **N:1 VLAN for 1:1 VLAN model**

- **ISG Sessions**
- **MPLS/IP, IP Multicast**
- **MPLS VPN, Multicast VPN (w/ HD-VRF)**

- **Efficient Access**
- **Large Scale Equal Access Aggregation**
- **Wholesale Intelligent Edge**
- **Multiservice Core**

- **Integrated Edge**
- **Distribution**
- **BNG**
- **Core**

- **DSL, PON, Ethernet, WiMAX**
- **ISG**
- **MPLS**
- **ISG**
- **MPLS**

© 2007 Cisco Systems, Inc. All rights reserved.
ISG
Intelligent Services Gateway
Intelligent Services Gateway
Dynamic Subscriber and Service Management

- It enables a Cisco network device to be a Policy Enforcement Point (PEP) (and optionally PDP)

- It is an IOS functional component that enables:
  - IP and PPPoE session management and control
  - IP service flow management and control
  - Local and remote Session Control Policies with event and condition based enforcement:
    - AAA, Transparent or Portal based Logon, Logoff, Timeouts, Time Volume Prepaid
  - Local and remote Traffic Control Policies with event and condition based enforcement:
    - QOS, ACLs, L4 redirect
  - Local and remote Network Control Policies with event and condition based enforcement:
    - L2TP selection, VRF selection and transfer
ISG Subscriber Session Data Plane

- **Session-Features**: Apply to the entire session e.g. per-session-ACL, Policing, H-QOS, Accounting, L4 redirect
- **Traffic Classification**: Apply to the entire session e.g. per-session-ACL, Policing, H-QOS, Accounting, L4 redirect
- **Flow-Classification**: Apply to the classified flow (a portion of the entire session data)
- **Network Service**: Forwarding (at L2, e.g. L2TP) or Routing (L3, e.g. connection to a VRF) Mutually exclusive
ISG Internal and External Policy Control

Business Policy Decisions: Centralized

Event

Policy Decision Point (PDP)

ISG takes role of PDP and PEP: Communication to external Server not required/optional

Central Services (Application & Policy)
Multiple Layers through ISP SP etc.

ISG Network Element Services (Access/Aggregation)

Event

Signaling/Network Policy Decisions: Distributed

Data

Identification/Classification (ACL)

Flow Feature

Network Service (route/forward)

ISG takes role of PDP and PEP: Communication to external Server not required/optional

Central Services (Application & Policy)
Multiple Layers through ISP SP etc.
ISG Local Policy Control

Control Policy
Associate Events and Conditions to an ordered list of Actions

<table>
<thead>
<tr>
<th>Control Class: List of Actions</th>
<th>Condition</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Disable Service B</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Enable Service A</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Class: List of Actions</th>
<th>Condition</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Enable Service X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Enable Service Y</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Take Action R</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Class: List of Actions</th>
<th>Condition</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1. Enable Service PBHK</td>
<td>20 authorize aaa password lab identifier circuit-id</td>
</tr>
<tr>
<td></td>
<td>2. Take action AAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Enable Service L4R</td>
<td>40 set-timer IP_UNAUTH_TIMER 5</td>
</tr>
<tr>
<td></td>
<td>4. Take action: Set Timer</td>
<td></td>
</tr>
</tbody>
</table>

policy-map type control SUBSCRIBER_RULE
  class type control always event session-start
    10 service-policy type service name PBHK
    20 authorize aaa password lab identifier circuit-id
    30 service-policy type service name L4R
    40 set-timer IP_UNAUTH_TIMER 5
  !
  class type control always event account-logon
    10 authenticate aaa list IP_AUTH_LIST
    20 service-policy type service unapply name L4R
  !
  class type control CND_U event timed-policy-expiry
    10 service disconnect
  !
ISG Dynamic Interface for Session and Service Control

RADIUS CoA, SGI (SOAP/BEEP)...

Dynamic Session Interface
- Session logon/logoff
- View Service List
- Service logon/logoff
- View Session status
- View System messages
- Feature Change

ISG features controllable by RADIUS
Service polices including traffic policies, L4 redirect, Subscriber ACL, Idle Timer, Session Timer, QoS, Session/Service Accounting, Pre-paid
### ISG – Key Functionality

<table>
<thead>
<tr>
<th>Service Selection / Self-Care</th>
<th>Reduced CAPEX and OPEX for mass customization of broadband services</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Flexible Accounting</strong></td>
<td>Per session and per service accounting, QoS Accounting, Pre-paid (volume), Pre-paid (Time-Based), Tariff-Switching (Pre-Paid and Post-paid)</td>
</tr>
<tr>
<td><strong>Authentication / Authorization</strong></td>
<td>L4 redirect for Web-Based Authentication, Transparent Auto Logon, PPP Authentication</td>
</tr>
<tr>
<td><strong>Dynamic Policy Push</strong></td>
<td>Policies for session bandwidth, security and accounting that can be pushed dynamically in real time while session is still active – using standardized protocols (e.g. RADIUS, RFC3576 CoA)</td>
</tr>
<tr>
<td><strong>Flexible Session Type</strong></td>
<td>PPP and IP-Sessions - using different session initiators; access protocol agnostic</td>
</tr>
<tr>
<td><strong>Policy based rules – “Control Policy”</strong></td>
<td>Event triggered conditional actions: Association of actions based on events</td>
</tr>
<tr>
<td><strong>“Domain Switching”</strong></td>
<td>Map user to VRF Dynamic VPN Selection</td>
</tr>
<tr>
<td><strong>MPLS integration – VRF-Switching</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Multidimensional Identity</strong></td>
<td>Policy determination based on all aspects of subscriber identity</td>
</tr>
<tr>
<td><strong>Timeouts</strong></td>
<td>Idle Timeout, Session and Service Timeouts</td>
</tr>
<tr>
<td><strong>Conditional debugging</strong></td>
<td>Debugging based on any subscriber, service or any other identifier</td>
</tr>
</tbody>
</table>
ISG IP Session Models
ISG IP Sessions Models

ISG IP Sessions:
- L2 or L3 (routed) connected sessions

ISG IP Session Creation:
- **RADIUS Access Request**: For routed IP subscribers, a new IP session is triggered by the RADIUS Access Request while ISG acts as RADIUS proxy.
- **Unclassified source IP address**: For routed IP subscribers, a new IP session is triggered by the appearance of an IP packet with an unclassified source IP address.
- **DHCP DISCOVER**: For Layer 2 connected IP subscribers, a new IP session is created based on DHCP Discover, while ISG acts as a DHCP relay or server.
- **Unclassified source MAC address**: For Layer 2 connected IP subscribers, a new IP session is triggered by the appearance of an IP packet with an unclassified source MAC address.

ISG IP Sessions Termination:
- **DHCP IP Sessions**: DHCP RELEASE or lease expiry.
- **RADIUS IP Sessions**: RADIUS Accounting-Stop (for RADIUS proxy operation).
- **Any IP sessions models**: Session Timeout, Account Logoff, ARP/ICMP/(BFD) keepalives timeout.
ISG IP Session

Subscriber Session = IP host

- Defined by a flow of traffic going to and from a subscriber IP address
- Configurable on logical (dot1q or QinQ) interfaces
- Session creation by FSOL* IP Packet, RADIUS proxy or DHCP relay
- Session end defined by DHCP lease, RADIUS Accounting Stop or timeout
- 1:n relationship between Interface and IP Session
- When using ISG/RADIUS for provisioning, features are applied to the session itself, not the interface
- Classification based on MAC, IP
- L2 connected or routed from first Aggregation device

Note: In case of a bridged CPE each IP host creates its own IP Session on the ISG gateway

*First Sign of Life
ISG IP Interface Session

Subscriber Session = IP Interface

IP interface session

- Defined by all traffic to and from a subscriber subinterface
- Configurable on logical Interfaces (dot1q or QinQ)
- 1:1 Mapping between Session and Interface
- Session initiation is at provisioning time (same for acct. start)
- Session end is at de-provisioning time (same for acct. stop)
- Dynamic RADIUS based features provisioning and changes
ISG IP Subnet Session

Subscriber Session = IP Subnet

IP subnet session
- Configurable on Physical or Logical (dot1q or QinQ)
- Represents a subscriber IP subnet
- IP subnet sessions are supported as routed IP subscriber sessions only.
- IP subnet sessions are created the same way as IP sessions
  (except that when a subscriber is authorized or authenticated and the Framed-IP-Netmask attribute is present in the user or service profile, ISG converts the source-IP-based session into a subnet session with the subnet value in the Framed-IP-Netmask attribute=
Notes:

1b. Note: We assume DHCP DISCOVER is the first sign of life. Conditions may arise such as a user leaves his previous session with a long lease still outstanding. When he returns, his PC will just send packets using the existing address. The first IP packet will be treated as the session-start event, the system will correlate the MAC address (if available) against cached DHCP information and then continue as shown.

3b. The AAA server knows which port the user is connected to and will use the Opt-82 information to successfully authorize the User. This results in TAL-like (transparent auto logon) behavior.

PPPoE sessions have a similar model.
Notes:

1a. Note: We assume the first IP packet is the first sign of life and the ISG gateway is configured for Transparent Auto Logon. The ISG session is created and RADIUS authorization is initiated.

3b. The subscriber profile in the RADIUS server is defined based on the static IP address allocated to that subscriber. This results in TAL-like (transparent auto logon) behavior.
Notes:

1a. We assume the first IP packet is the first sign of life.
2. The IP Session is created with a basic set of policies that are granting access to the authentication portal and L4-redirect to that portal.
4. Redirect User to Portal to have him input his credentials and service preference. Set a timer which will remove the session if the authentication is not successful (avoid accumulating state).
12. Accounting record informs AAA server about user’s identity (IP address and user name). Note: Accounting messages need to be understood as state/event notifications, not just charging information.
Notes:

0. Subscriber is logged on and portal displays authorized service profile info

1a. User requests addition of a new service (video) to their profile.

1b. Back-end process request/payment/subscription info and updates subscriber profile. Portal displays result

2. User activates new service.

3. Portal sends new service activate CoA to ISG

4. ISG requests service profile from Radius

5. User accesses service page (after logon)

6. ISG activates service

7. CoA ACK

8. Portal displays authorized service profile page

9. CoA Service Activate

10. RADIUS Access Request Username := ServiceX

11. RADIUS Access Accept

12. ISG activates service

13. CoA ACK

14. Portal displays authorized service profile page

15. CoA Service Activate

16. RADIUS Access Request Username := ServiceX

17. RADIUS Access Accept

18. ISG activates service

19. CoA ACK

20. Portal displays authorized service profile page

21. CoA Service Activate

22. RADIUS Access Request Username := ServiceX

23. RADIUS Access Accept

24. ISG activates service

25. CoA ACK

26. Portal displays authorized service profile page

27. CoA Service Activate

28. RADIUS Access Request Username := ServiceX

29. RADIUS Access Accept

30. ISG activates service

31. CoA ACK

32. Portal displays authorized service profile page

33. CoA Service Activate

34. RADIUS Access Request Username := ServiceX

35. RADIUS Access Accept

36. ISG activates service

37. CoA ACK

38. Portal displays authorized service profile page

39. CoA Service Activate

40. RADIUS Access Request Username := ServiceX

41. RADIUS Access Accept

42. ISG activates service

43. CoA ACK

44. Portal displays authorized service profile page

45. CoA Service Activate

46. RADIUS Access Request Username := ServiceX

47. RADIUS Access Accept

48. ISG activates service

49. CoA ACK

50. Portal displays authorized service profile page

51. CoA Service Activate

52. RADIUS Access Request Username := ServiceX

53. RADIUS Access Accept

54. ISG activates service

55. CoA ACK

56. Portal displays authorized service profile page

57. CoA Service Activate

58. RADIUS Access Request Username := ServiceX

59. RADIUS Access Accept

60. ISG activates service

61. CoA ACK

62. Portal displays authorized service profile page

63. CoA Service Activate

64. RADIUS Access Request Username := ServiceX

65. RADIUS Access Accept

66. ISG activates service

67. CoA ACK

68. Portal displays authorized service profile page

69. CoA Service Activate

70. RADIUS Access Request Username := ServiceX

71. RADIUS Access Accept

72. ISG activates service

73. CoA ACK

74. Portal displays authorized service profile page

75. CoA Service Activate

76. RADIUS Access Request Username := ServiceX

77. RADIUS Access Accept

78. ISG activates service

79. CoA ACK

80. Portal displays authorized service profile page

81. CoA Service Activate

82. RADIUS Access Request Username := ServiceX

83. RADIUS Access Accept

84. ISG activates service

85. CoA ACK

86. Portal displays authorized service profile page

87. CoA Service Activate

88. RADIUS Access Request Username := ServiceX

89. RADIUS Access Accept

90. ISG activates service

91. CoA ACK

92. Portal displays authorized service profile page
PPP to IP Sessions Evolution
Experience very similar to former PPP

- Subscriber Identification/Authentication
- Subscriber Isolation
- Identify Line ID (ATM VC/VP), PPPoE Tag
- IPCP
- Keepalives
- Service Selection
- Session and Service Accounting
- Start Session
- Stop Session
- Session Identification
- Datagram Transport
- RADIUS Authorization, Portal Logon
  - L3: ISG, ACLs, VRFs
  - L2: VLAN, private VLAN
- DHCP
  - DHCP opt. 82, vMAC
  - VLAN (802.1q, 802.1ad)
- ICMP, ARP
- Policy events (authorization, portal based, prepaid…)
- RADIUS
  - Provisioned, DHCP, MAC, IP (subnet), RADIUS
  - Session and/or Keepalives Timeout
  - DHCP/RADIUS session stop, Logoff
  - VLAN Interface, Mac, IP (subnet)
  - IP/Ethernet

Some open considerations…

Advanced Authentication (CHAP, PAP, EAP based)
Consistent and coordinated session lifecycle on the client and server

© 2007 Cisco Systems, Inc. All rights reserved.
Additional Considerations
For Transparent PPPoE to IPoE Migration
IP sessions Authentication for Transparent Evolution from PPPoE to IPoE

- **Target:**
  Use the PPPoE authentication models to avoid operational impact

- **Requirements:**

  - **The authentication must be secure**
    - Client credentials are sent based on a secure encryption scheme
  
  - **The authentication must be before IP address allocation**
    - Ensures entitlement to the service
    - Ensures safe and predictable IP address usage
    - Ensures predictable legal intercept for the client traffic
    - Ensures that any attacks are launched by known individuals

  - **The authentication process must accommodate clients that can’t perform authentication**

  - **The authentication process must rely on standards protocols and not disrupt or change existing protocols**

- **Standardization Direction:**

  Started efforts in IETF for defining the DHCP authentication models
**DHCP-AUTH as “drop-in” for PPPoE**
draft-pruss-dhcp-auth-dsl-02.txt (Alternative 1)

- Use existing DHCP message set
- Reverse Authentication and other Auth Protocols (e.g. EAP) not supported
- All Attributes are mapped from RADIUS including IP address or Pool
Enhanced DHCP-Auth – For EAP, CHAP server auth etc.
draft-pruss-dhcp-auth-dsl-02.txt (Alternative 2)

Expands capabilities of “Alternative 1”:
- supports CHAP server authentication
- supports EAP and with that more advanced methods for authentication

Requires:
- A new message
- DHCP message size >= 1604 for use with EAP message option (RFC 2132 – max DHCP message size option)
IP sessions Keepalives for Transparent Evolution from PPPoE to IPoE

- **IP sessions considerations**
  - IP flows are connection-less
  - Neither Ethernet nor IP have a well-defined, built-in session life cycle

- **IP Sessions need to be defined in respect of a session lifecycle**
  - IPoE session start/stop can be inferred from:
    - data-plane: e.g. 1st reception packet/frame from an unclassified source (IP/MAC address) and idle timeout
    - or
    - control-plane: e.g. by performing/witnessing a successful DHCP lease and lease expiration/release (similarly with RADIUS)

- **In addition, there has to be a keepalives mechanism that allows detection of a session failure, resp. failed connectivity**

- **An IP Session keepalives mechanism needs to be implemented on client and server in order to obtain PPP like behavior**
  - By the server: to enable accurate session lifecycle and accounting
  - By the IP client: to enable a similar inter server redundancy model

- **DSLFWT-146 has specified several keepalives mechanisms for IP sessions, in the server and client: ARP, BFD based**
Access Node Dual-homing
IPoE Session Re-Initiation

1. Residential STB
   +DHCP Discover
   Access Node
   +DHCP Discover
   BNG
   I/F (ISG)

2. Residential STB
   +DHCP Offer
   Access Node
   +DHCP Offer
   BNG
   I/F (ISG)

3. Residential STB
   +DHCP Request
   Access Node
   +DHCP Request
   BNG
   I/F (ISG)

4. Residential STB
   +DHCP Ack
   Access Node
   +DHCP Ack
   BNG
   I/F (ISG)

For IP routed sessions, FSOL is an RADIUS AR or new IP flow.
IPoE Session with a connection-oriented concept with built-in lifecycle management

- Session failure can be detected by means of session keepalives (ICMP, ARP, BFD)
- Both, client and server (BNG) will be aware of session failure and terminate the session context
- Client will/may re-initiate a new session upon session failure and thereby create a new session with a standby BNG

For IP routed sessions, keepalives are based on BFD or ICMP
Conclusion
PPP to IP Journey....
A Natural But Simple Evolution

- Carrier Ethernet deployments with IPTV services and Ethernet based access options are driving the migration from PPP to IP
- This migration has to be transparent for the service provider from functional and operational aspects
- There are various service delivery models that drive different IP session deployment models

- Cisco Intelligent Services Gateway enables the same services and operational behaviour for PPPoE and the various IP sessions models
- Standardization efforts are in place to fine tune the remaining functional aspects for full operational consistency

- In conclusion the migration from PPP to IP can be considered a natural and simple evolution …