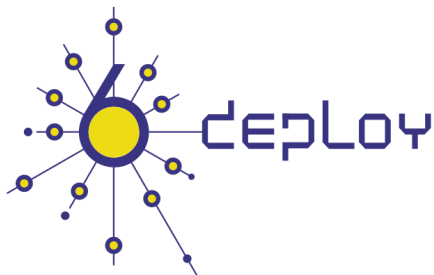


Broadband Deployment with IPv6


APNIC
Christchurch, NZ
August 2008

Jordi Palet (jordi.palet@consulintel.es)



Contenido

1. Auto configuration, DHCPv6 and Prefix Delegation
2. IPv6 en broadband technologies



1. Autoconfiguration, DHCPv6 and Prefix Delegation



1.1 Autoconfiguration

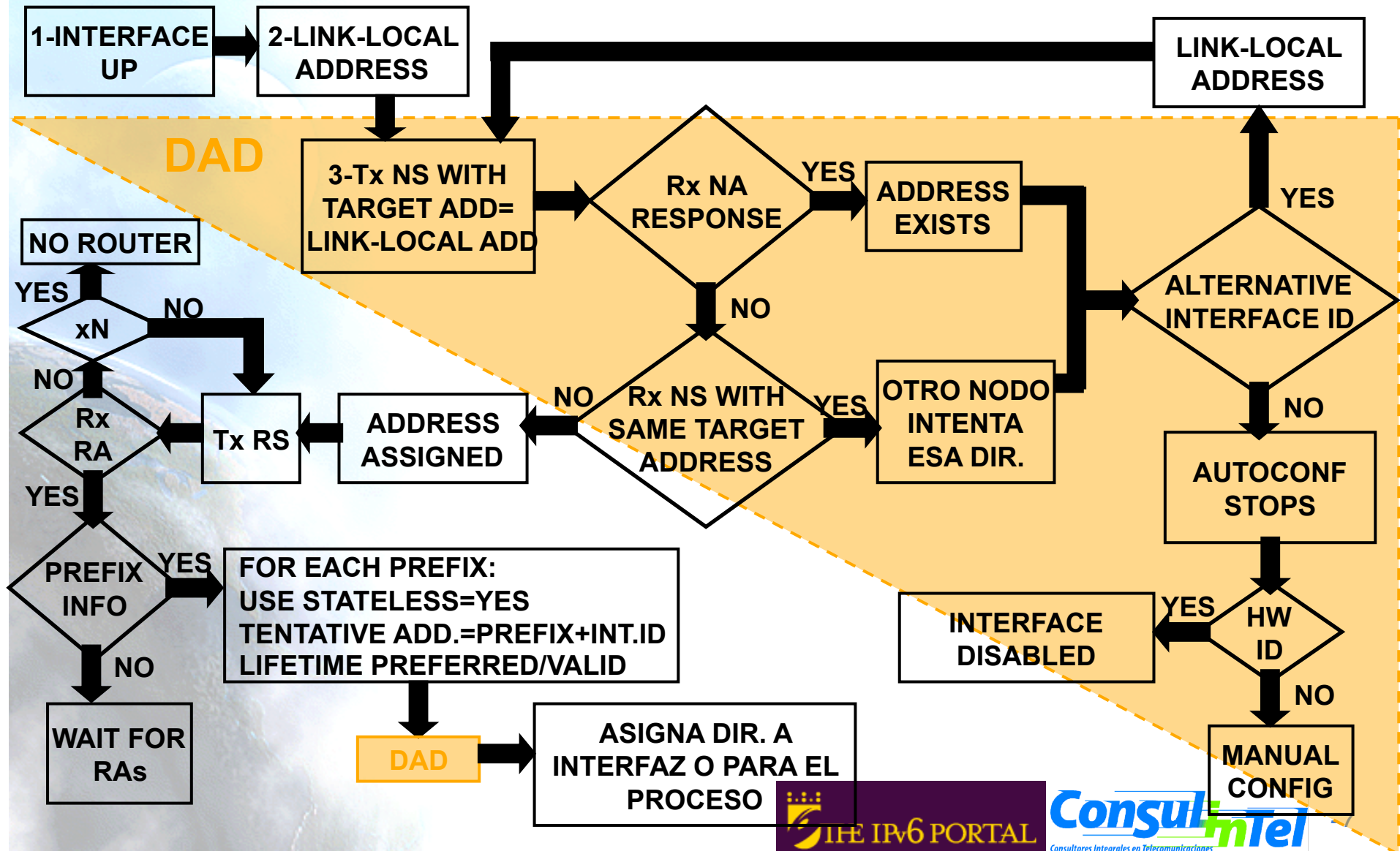
RFC2462

- The document specifies the steps a host takes in deciding how to autoconfigure its interfaces in IPv6.
- The autoconfiguration process includes creating a link-local address and verifying its uniqueness on a link, determining what information should be autoconfigured (addresses, other information, or both), and in the case of addresses, whether they should be obtained through the stateless mechanism, the stateful mechanism, or both.
- IPv6 defines both a stateful and stateless address autoconfiguration mechanism.
- Stateless autoconfiguration requires no manual configuration of hosts, minimal (if any) configuration of routers, and no additional servers.

Stateless or Serverless Autoconfiguration

- Stateless mechanism allows a host to generate its own addresses using a combination of locally available information and information advertised by routers.
- Routers advertise prefixes that identify the subnet(s) associated with a link.
- Hosts generate an "interface identifier" that uniquely identifies an interface on a subnet, locally generated, e.g., using MAC address.
- An address is formed by combining the both.
- In the absence of routers, a host can only generate link-local addresses.
- Link-local addresses are sufficient for allowing communication among nodes attached to the same link.

Stateless autoconfiguration



Stateful Autoconfiguration

- Hosts obtain interface addresses and/or configuration information and parameters from a server.
- Servers maintain a database that keeps track of which addresses have been assigned to which hosts.
- Stateless and stateful autoconfiguration complement each other.
- Both stateful and stateless address autoconfiguration may be used simultaneously.
- The site administrator specifies which type of autoconfiguration to use through the setting of appropriate fields in Router Advertisement messages.

Address Life Time

- IPv6 addresses are leased to an interface for a fixed (possibly infinite) length of time, that indicates how long the address is bound to an interface.
- When a lifetime expires, the binding (and address) become invalid and the address may be reassigned to another interface elsewhere in the Internet.
- To handle the expiration of address bindings gracefully, an address goes through two distinct phases while assigned to an interface.
 - Initially, an address is "preferred", meaning that its use in arbitrary communication is unrestricted.
 - Later, an address becomes "deprecated" in anticipation that its current interface binding will become invalid.

Duplicate Address Detection

- To insure that all configured addresses are likely to be unique on a given link, nodes run a "duplicate address detection" algorithm on addresses before assigning them to an interface.
- The Duplicate Address Detection algorithm is performed on all addresses, independent of whether they are obtained via stateless or stateful autoconfiguration.
- The procedure for detecting duplicate addresses uses Neighbor Solicitation and Advertisement messages.
- Since host autoconfiguration uses information advertised by routers, routers will need to be configured by some other means. However, it is expected that routers will generate link-local addresses using the same mechanism.
- Routers are expected to successfully pass the Duplicate Address Detection procedure on all addresses prior to assigning them to an interface.

DNS configuration with Stateless autoconfiguration (1)

- Typically DNS server configuration in IPv6 nodes has been done by means of:
 - Manual configuration
 - DHCPv6 or DHCPv4 (in case of dual-stack nodes)
- However, this has some inconveniences in some environments:
 - Need to run two IPv6 protocols (Stateless autoconfiguration –RA-, DHCPv6)
 - Delay in obtaining the address of the DNS server when using DHCP
 - Impossibility of manual configuration and/or delay with DHCP when the node is located at wireless environments and attaching continuously to new networks
- It is possible to use DNS configuration based on RA as an alternative to provide the address of one or several DNS servers
 - An specific address in the RA packet is used
 - Recursive DNS Server (RDNSS)
 - It is possible to use this together with DHCPv6

DNS configuration with Stateless autoconfiguration (2)

- It works the same as the way the nodes use to learn the router or the /64 prefix in a LAN (RFC4862): IPv6 Stateless Address Autoconfiguration
- By means of the RDNSS option, nodes learn with a single packet exchange:
 - Network related configuration (/64 prefix)
 - Nearest DNS servers
- If DHCPv6 is also to be used, then Flag “O” of RA packet should be set
- The configuration of the RDNSS option in the routers is done:
 - Manually
 - Automatically by means of DHCPv6 (as client)



1.2 DHCPv6

DHCPv6

(RFC3315 - RFC4361)

- DHCP for IPv6 (DHCPv6) is an UDP client/server protocol designed to reduce the cost of management of IPv6 nodes in environments where network managers require more control over the allocation of IPv6 addresses and configuration of network stack parameters than that offered by “IPv6 Stateless Autoconfiguration”.
- DHCP reduces the cost of ownership by centralizing the management of network resources rather than distributing such information in local configuration files among each network node.
- DHCP is designed to be easily extended to carry new configuration parameters through the addition of new DHCP “options” defined to carry this information.

DHCPv6 Goals

- Is a mechanism rather than a policy.
- Is compatible with IPv6 stateless autoconfiguration.
- Does not require manual configuration of network parameters on DHCP clients.
- Does not require a server on each link.
- Coexists with statically configured, non-participating nodes and with existing network protocol implementations.
- DHCP clients can operate on a link without IPv6 routers present.
- DHCP will provide the ability to renumber network(s).
- A DHCP client can make multiple, different requests.
- DHCP will contain the appropriate time out and retransmission mechanisms to efficiently operate in environments with high latency and low bandwidth characteristics.

Basic DHCPv6 example

client



server



SOLICIT (FF02::1:2)



ADVERTISE



REQUEST/RENEW



REPLY



client



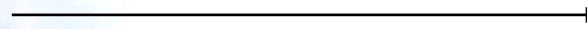
relay



server



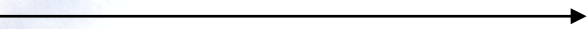
SOLICIT (FF02::1:2)



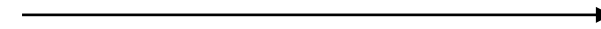
ADVERTISE



REQUEST/RENEW



REPLY





1.3 DHCPv6 Prefix Delegation

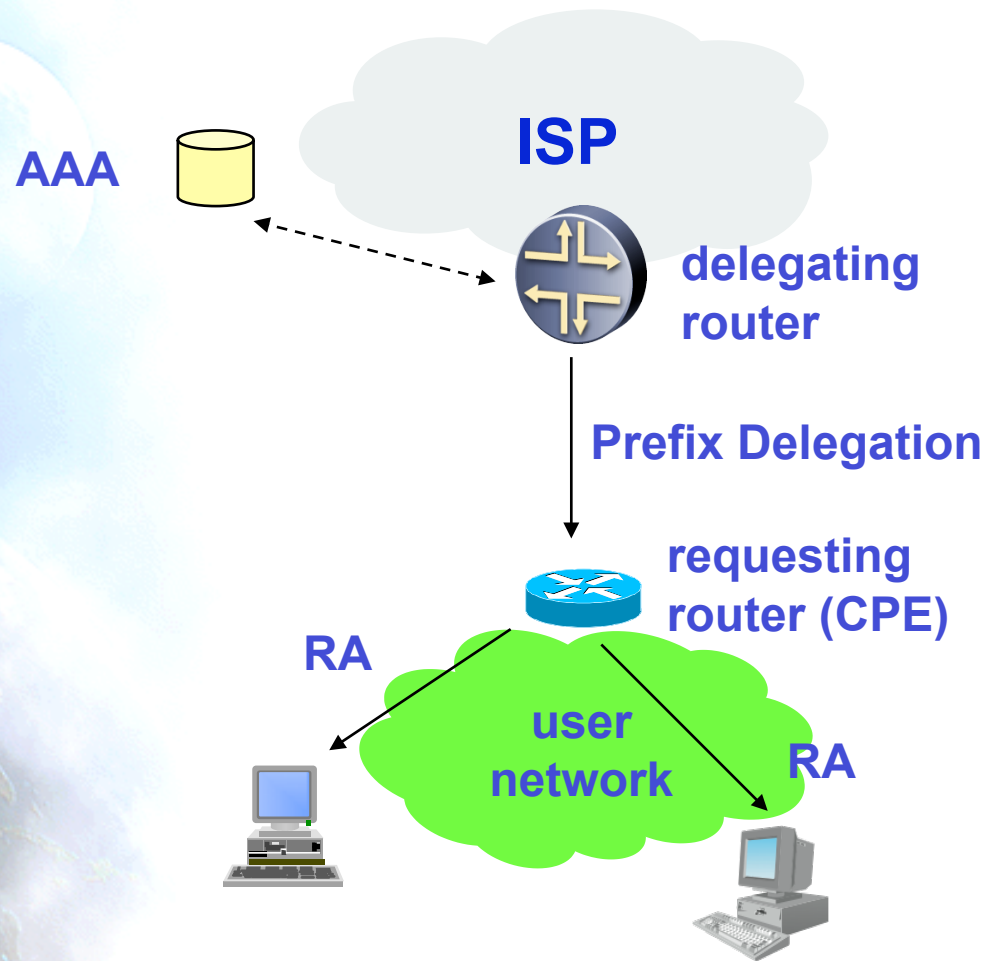
DHCPv6-PD (RFC3633)

- Provides to the authorized routers which need it, an automated mechanism for the delegation of IPv6 prefixes
- The delegating routers don't need to know the network topology of the solicitant routers
- The delegating routers don't need any information apart from the identity of the solicitant router
 - an ISP which assigns a prefix to the CPE which acts as the router

Details about DHCPv6-PD

- The solicitant router (Requesting Router, RR) needs authentication
- The RR profile can be stored within an AAA server
- The delegated prefix can be extracted from:
 - Customer profile, stored at the AAA server
 - List of prefixes (prefix pool)
- The delegated prefixes have life time, same as the IPv6 addresses in DHCPv6
- DHCPv6-PD doesn't provides a method to propagate the delegated prefix thru the user network
 - All the `::/64` prefixes which can be extracted from the delegated prefix, are assigned to the RR according to the configured policies
- DHCPv6 relays can be used in DHPv6-PD, exactly the same way as in DHCPv6

DHCPv6-PD Network Architecture



DHCPv6-PD basic example

client



requesting router



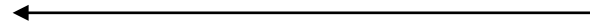
delegating router



SOLICIT (FF02::1:2, IA-PD)



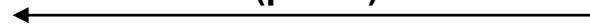
ADVERTISE



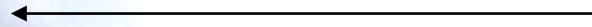
REQUEST/RENEW



REPLY (prefix)



Router Advertisement





2.

IPv6 in broadband technologies



2.2 IPv6 and broadband

IPv6 and Broadband (1)

- The deployment of broadband services extends the network infrastructure to many places
 - “Always on” xDSL connectivity at home
 - Network to the last mile
 - Allows connecting devices which previously were not connected (refrigerator, microwave oven, etc.)
 - Wireless “Hotspots”
 - Public locations
 - Allows connecting personal devices to access new services
 - 3G technology
 - Cellular phones for mobile users
 - GRID and middleware technologies
 - Allows connecting and controlling a large amount of devices
- As a result, broadband services increase exponentially the demand for IP addresses > IPv6

IPv6 and Broadband (2)

- The large amount of addresses available with IPv6 minimize the need for NAT
 - NAT create significant limitations to services
 - p2p
 - VoIP
 - Videoconferencing
 - Collaborative environments
- Each IPv6 device connected to the network is potentially a p2p device

IPv6 and Broadband (3)

- Broadband is the best solution to the demand of efficient means of communication which allow better data transfer rates
- This facilitates new services
 - E-health
 - E-government
 - E-work
 - E-education
 - etc.
- IPv6 provides the required tools to offer those services
 - Autoconfiguration
 - MIPv6
 - IPsec
 - QoS
 - Multicast

Choices for the deployment of IPv6 in Broadband

Choice	Pros	Cons
Native IPv6 with dedicated infrastructure	No impact in IPv4 services, more scalable	Possible high cost in big networks
Dual-stack with native IPv6 transport	Only requires updating part of the network	More resources required in dual-stack devices
IPv6-in-IPv4 tunnels	Minimal costs, only the tunnel-end-points are updated	Not scalable, more load in the end-point devices

¡ Choose native IPv6 !

- Native IPv6 provides better results in the medium-long term
- Dual-stack is a good way to start the IPv4 to IPv6 transition
- Tunnels only to be used when native IPv6 (dual-stack), is not feasible

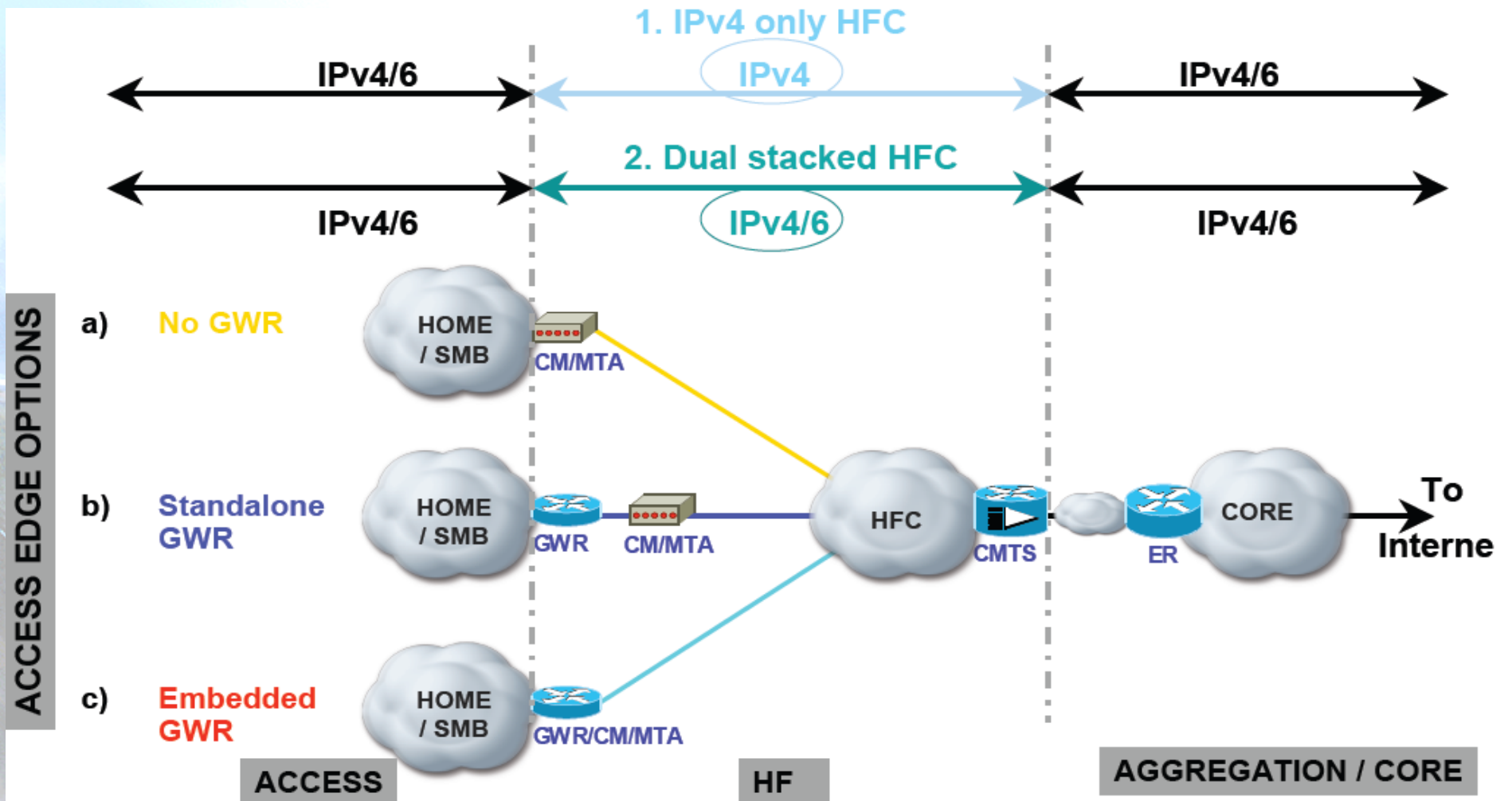


2.2.1 IPv6 in DOCSIS cable networks

DOCSIS network elements

- Cable (HFC) Plant
 - Hybrid Fiber Coaxial plant, used as the transport to carry the traffic to the subscriber
- Cable Modem Termination System (CMTS)
 - Located in the header or distribution hub, provides data connectivity between the Host/Cable Modem and other devices of the IP network
- Cable Modem (CM)
 - Modulator/Demodulator at the subscriber location to transport the data to/from the HFC
- Multimedia Terminal Adapter (MTA)
 - Transports VoIP to/from the subscribers
- Residential Gateway Router (GWR)
 - Provides level 3 services to the hosts
- Host
 - PC, laptop, device, etc. connected to the CM or the GWR
- Edge router (ER)
 - Border router connecting the CMTS to the core network. An ER can aggregate several CMTSs

IPv6 in DOCSIS

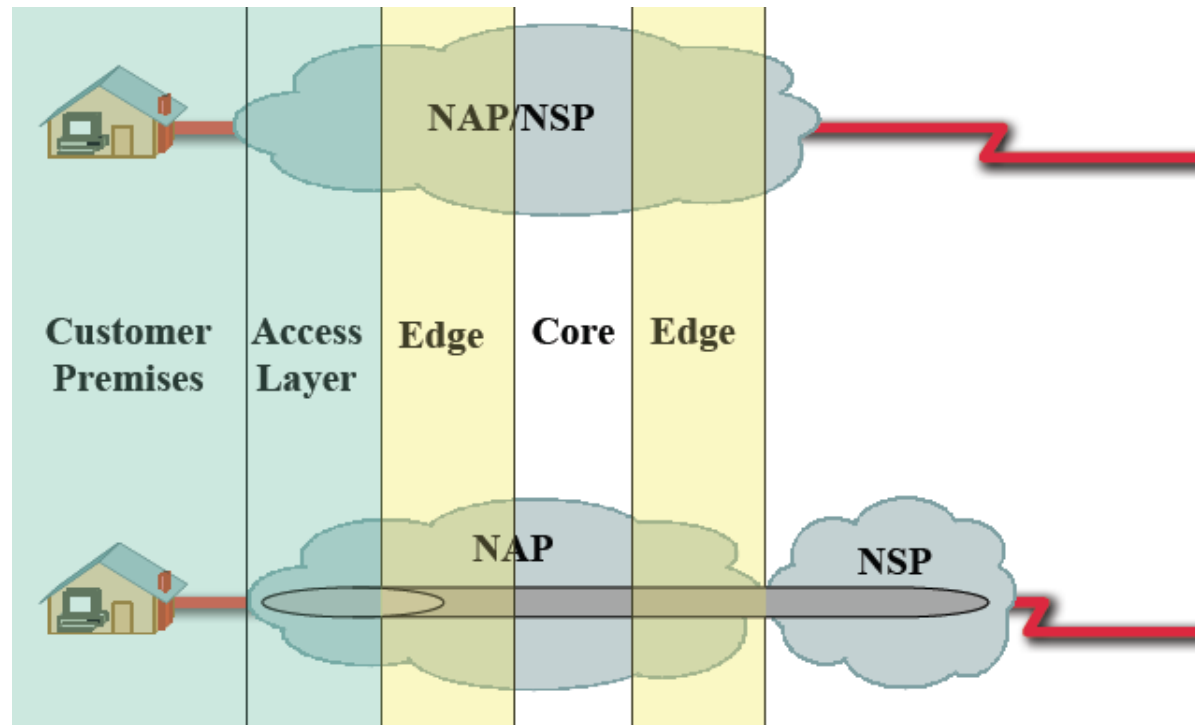




2.2.2 IPv6 in ADSL networks

ADSL broadband access models

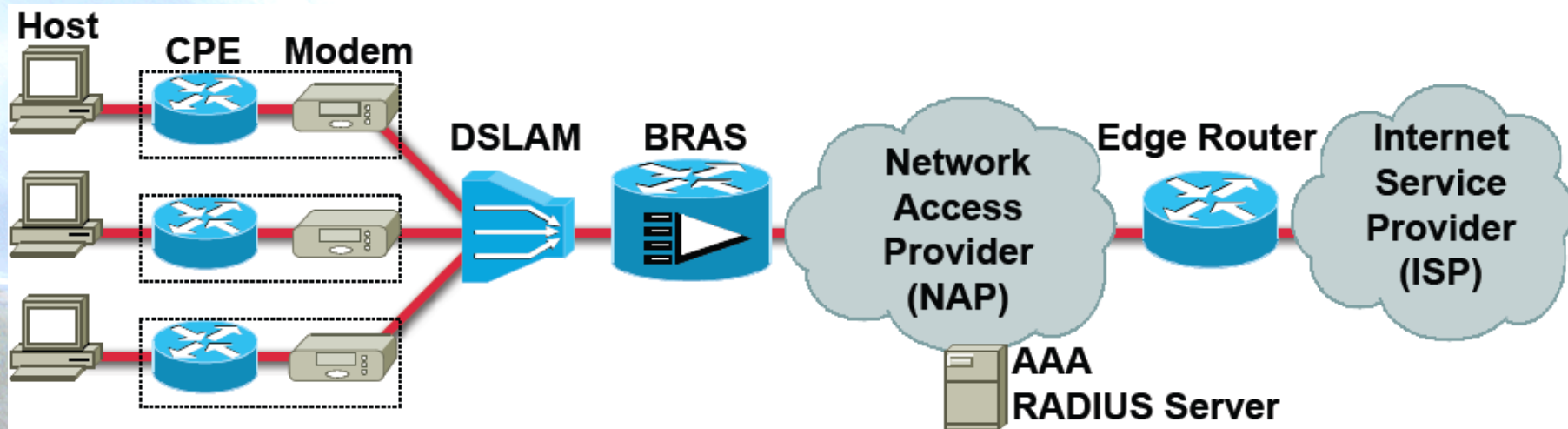
- **NAP = NSP**
 - Point-to-Point
 - PPP
 - Terminated Aggregation (PTA)
- **NAP # NSP**
 - Agregation L2TPv2 (LAA)



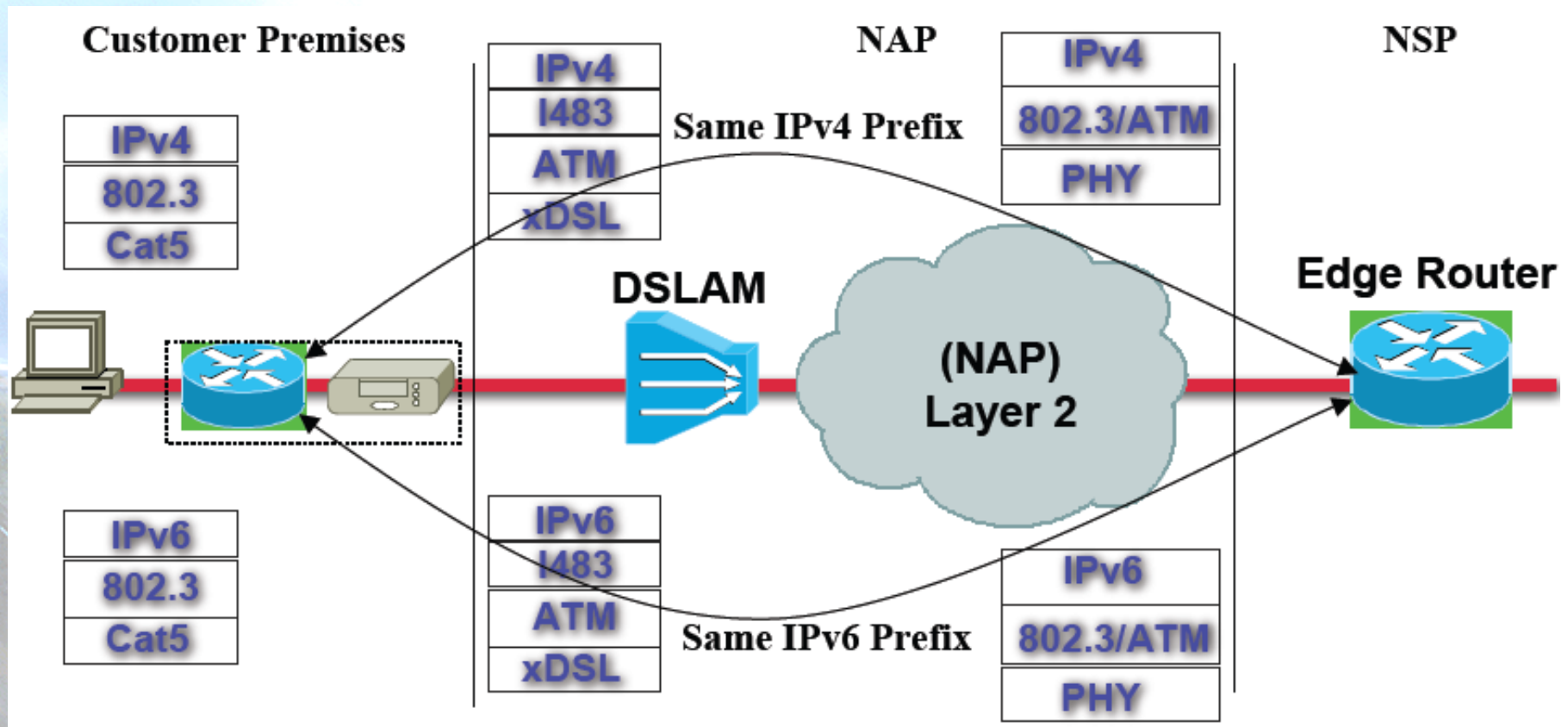
ADSL network elements

- Broadband Remote Access Server (BRAS)
- Digital Subscriber Line Access Multiplexer (DSLAM)
- DSL Modem
- Customer Premises Equipment (CPE)
- Host
- Edge Router (ER)

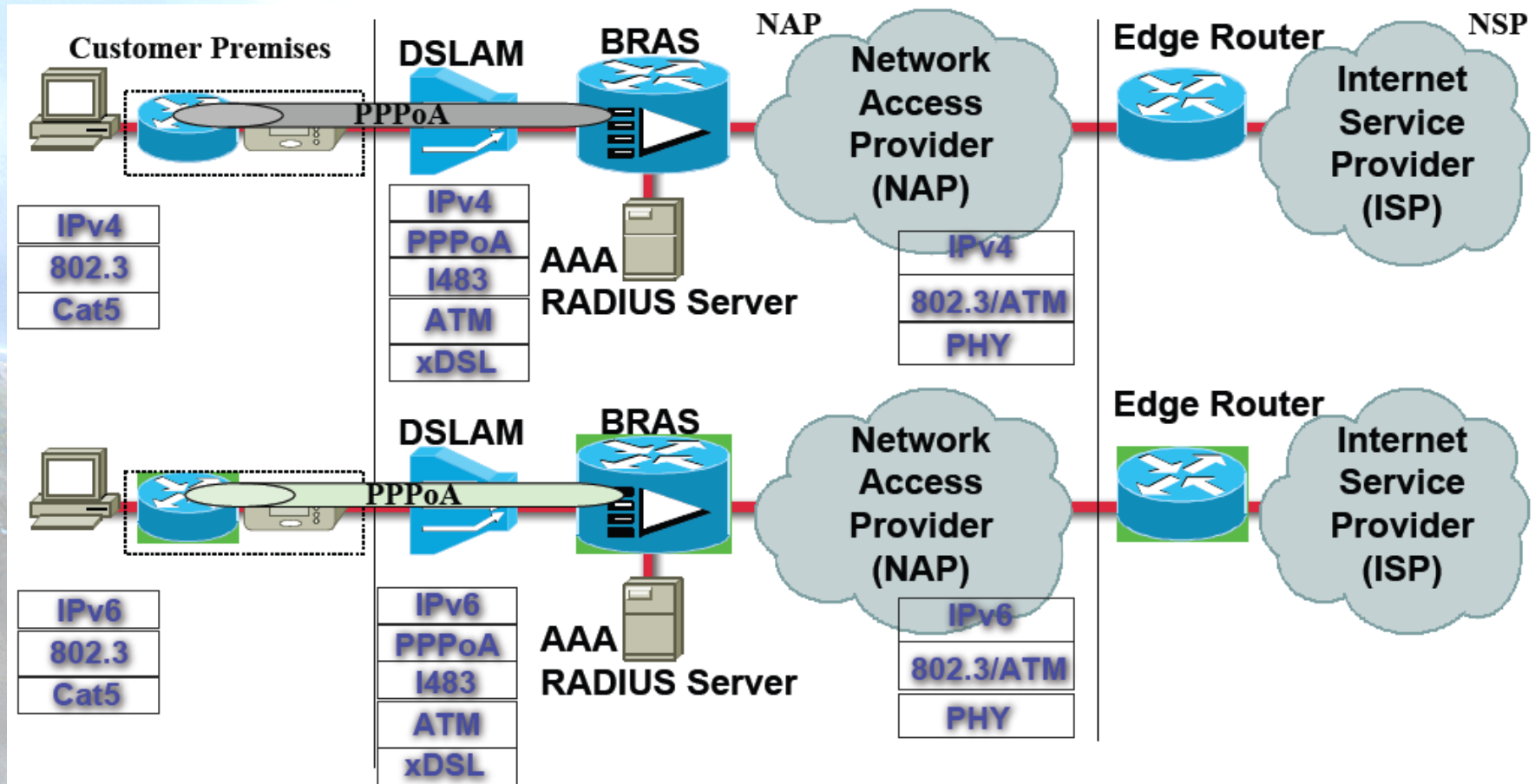
ADSL network basic topology



Point-to-point model

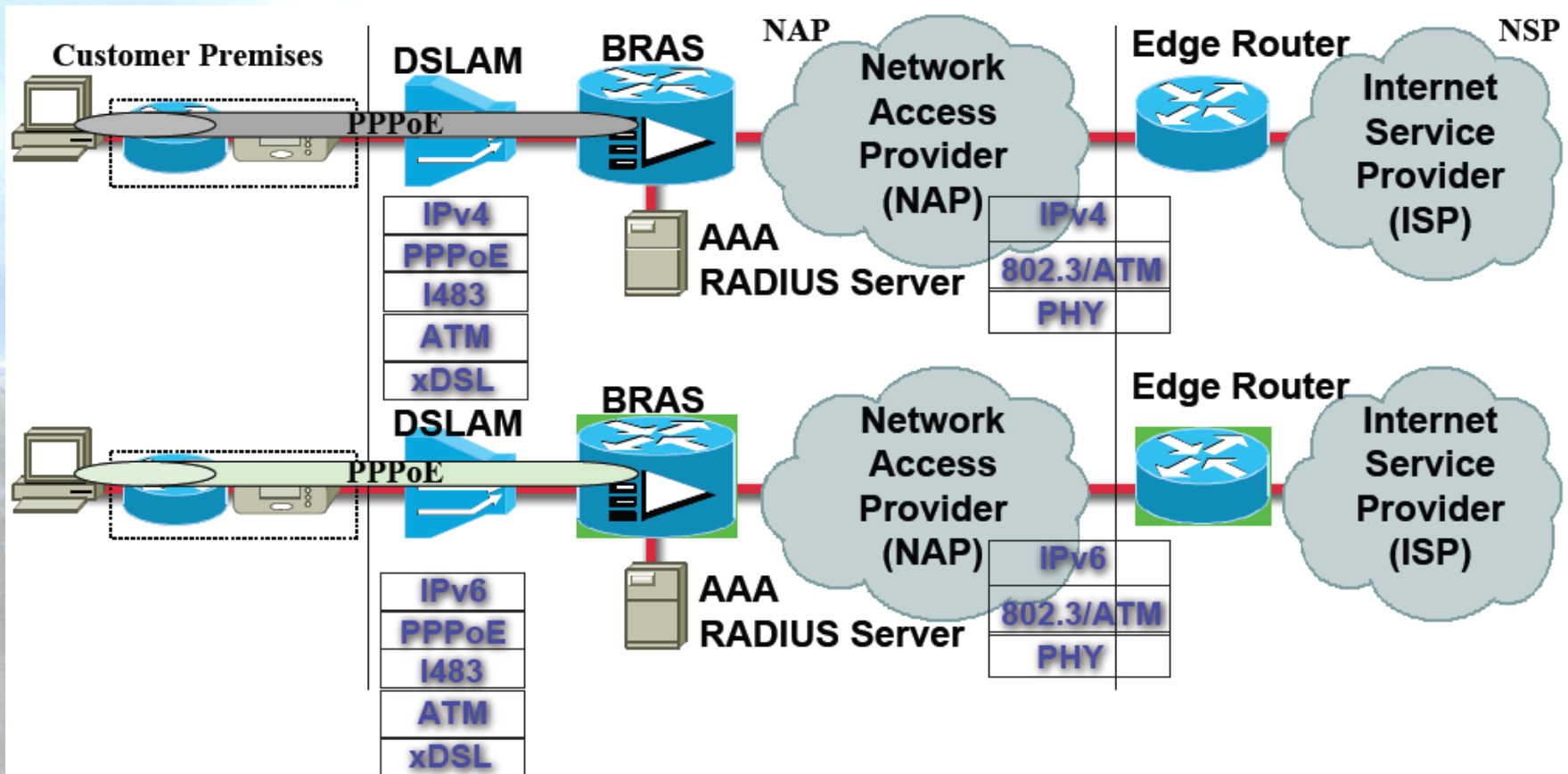


PPP Terminated Aggregation (PTA) – PPPoA Model



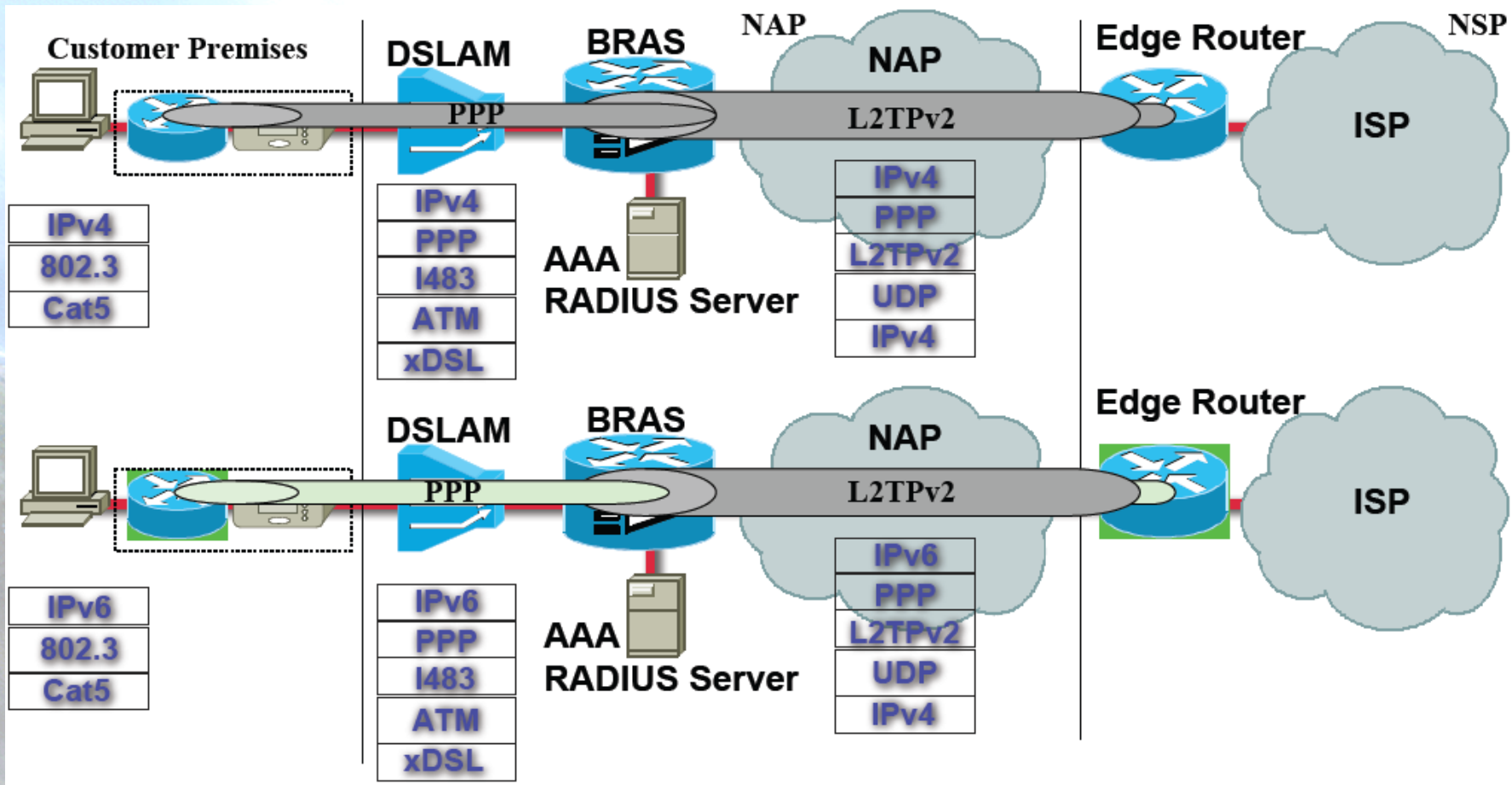
Note: Only a single PPPoA session for each PVC

PPP Terminated Aggregation (PTA) – PPPoE Model



Note: Multiple PPPoE for each PVC
 PPPoE sessions can be initiated by the hosts or the CPEs

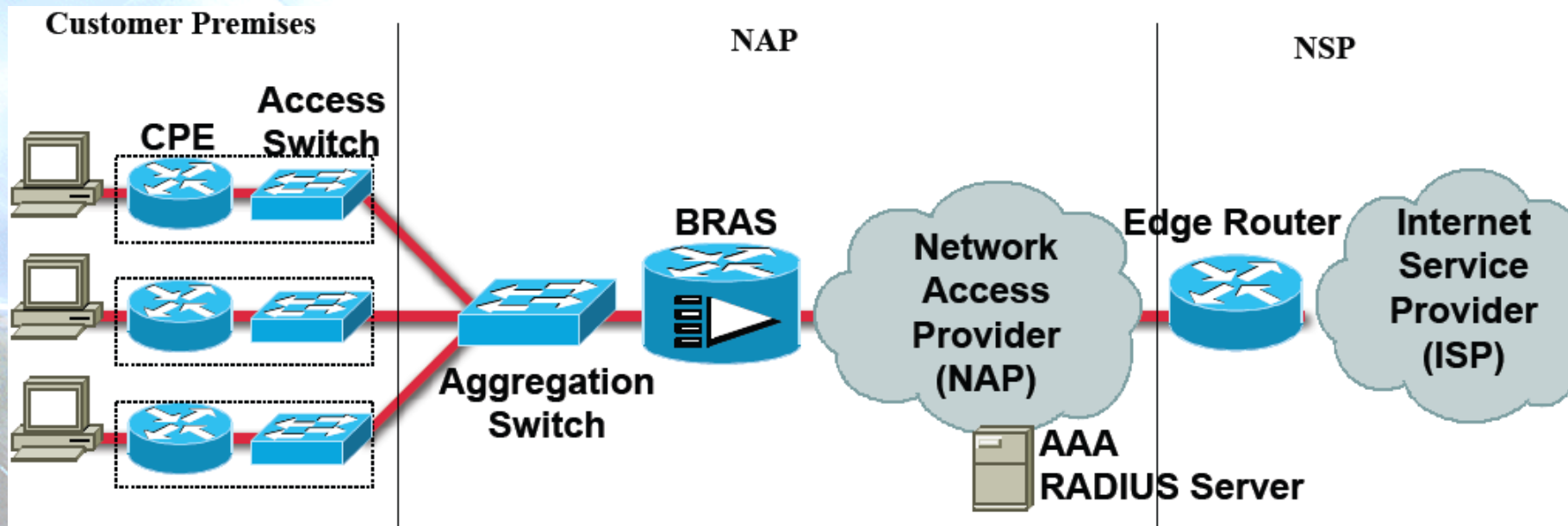
L2TPv2 Access Aggregation (LAA) Model





2.2.3 IPv6 in Ethernet networks

Broadband Ethernet basic topology



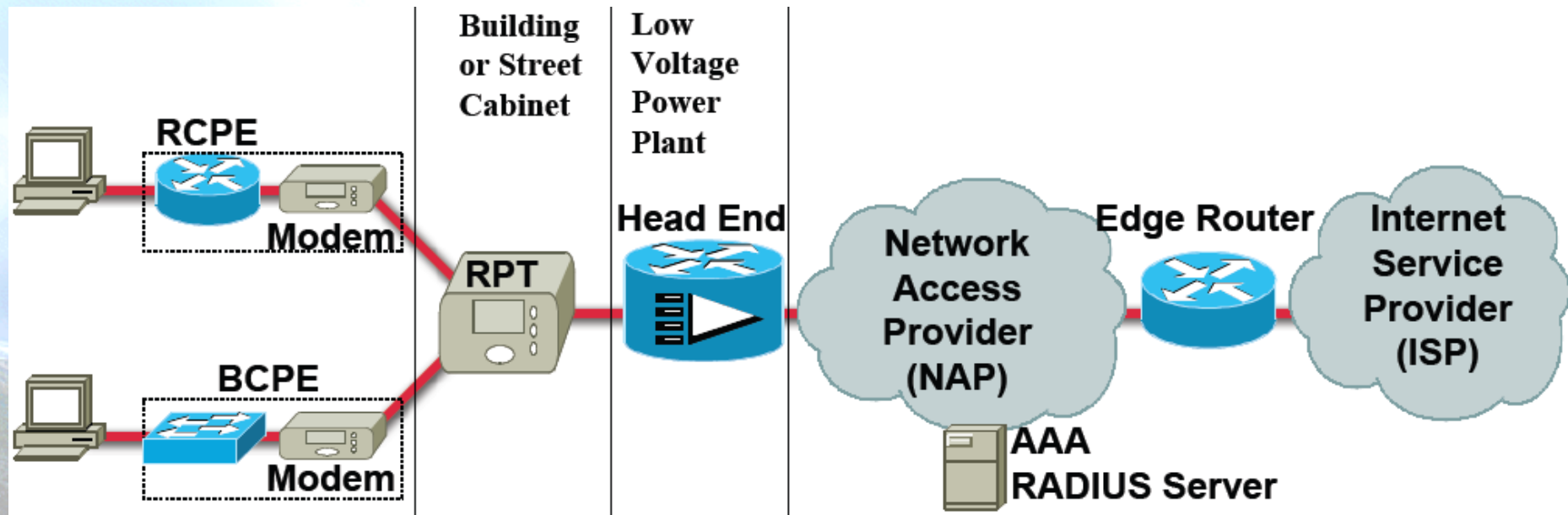
Models

- NAP = NSP
 - Point-to-point
 - PPP Terminated Aggregation (PTA)
- NAP ≠ NSP
 - L2TPv2 Aggregation (LAA)



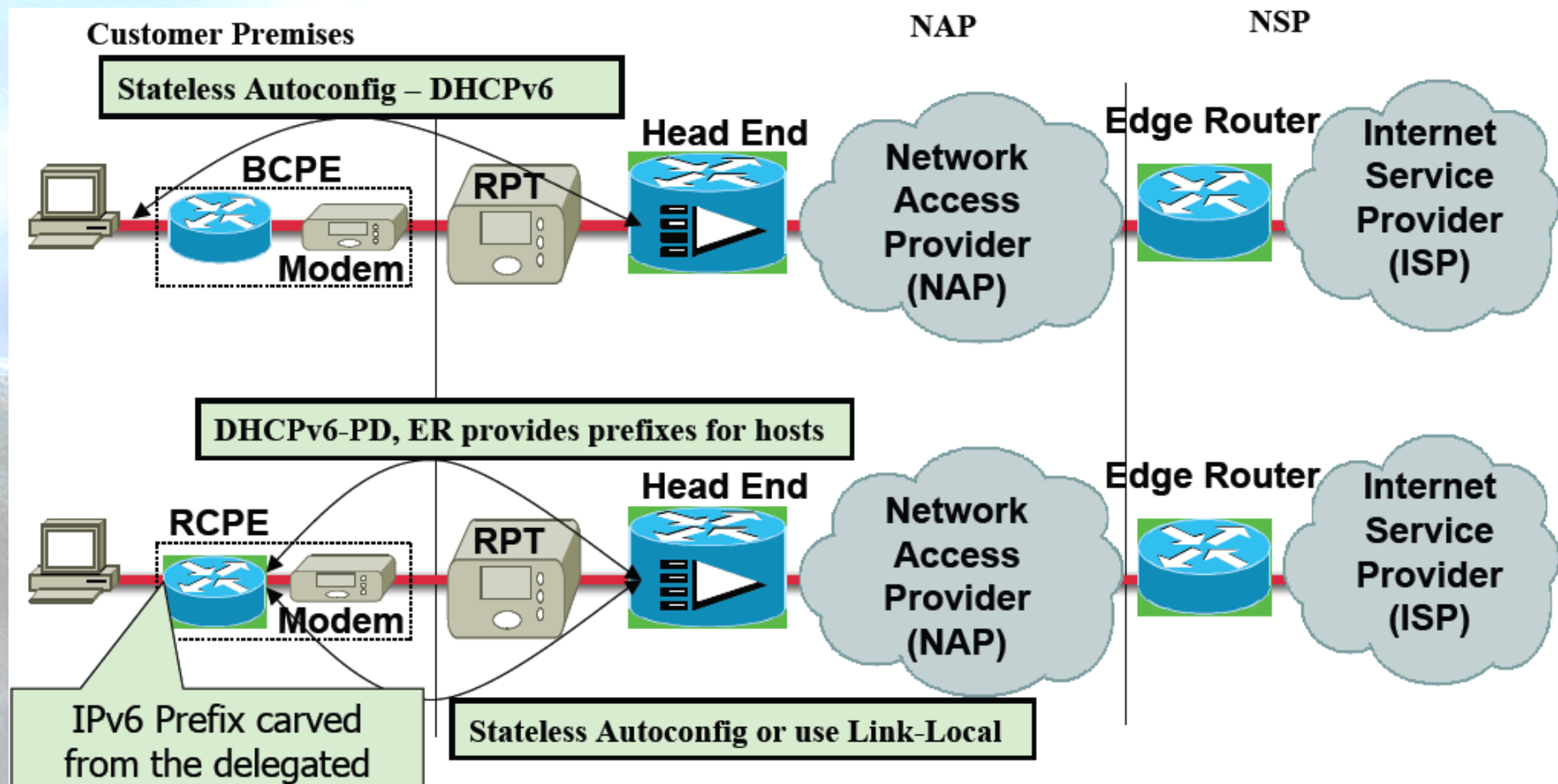
2.2.4 IPv6 in PLC/BPL networks

PLC network basic topology



Note: RPT is typically a level 2 device, but it can be a router in some cases

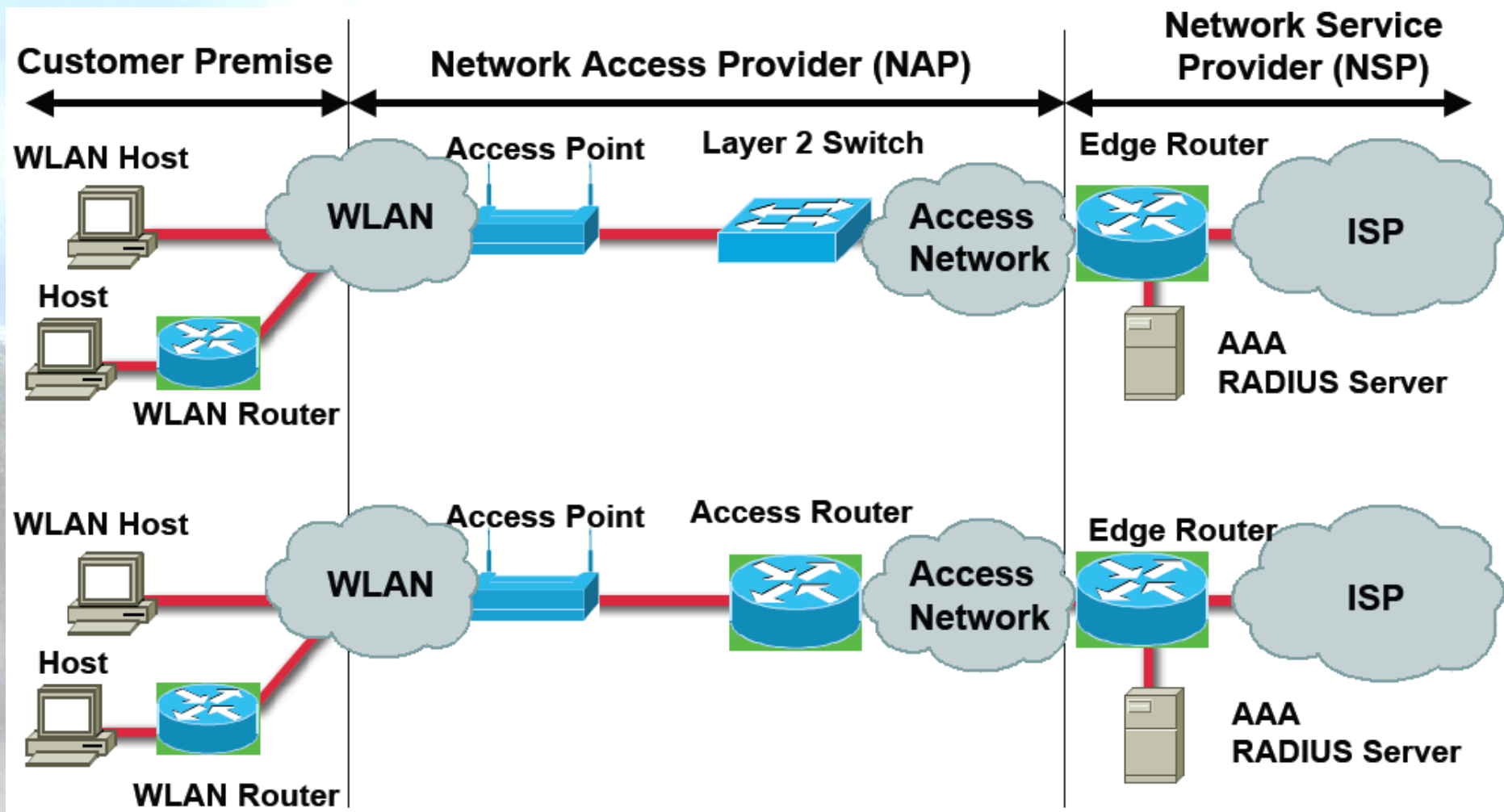
IPv6 in the PLC network



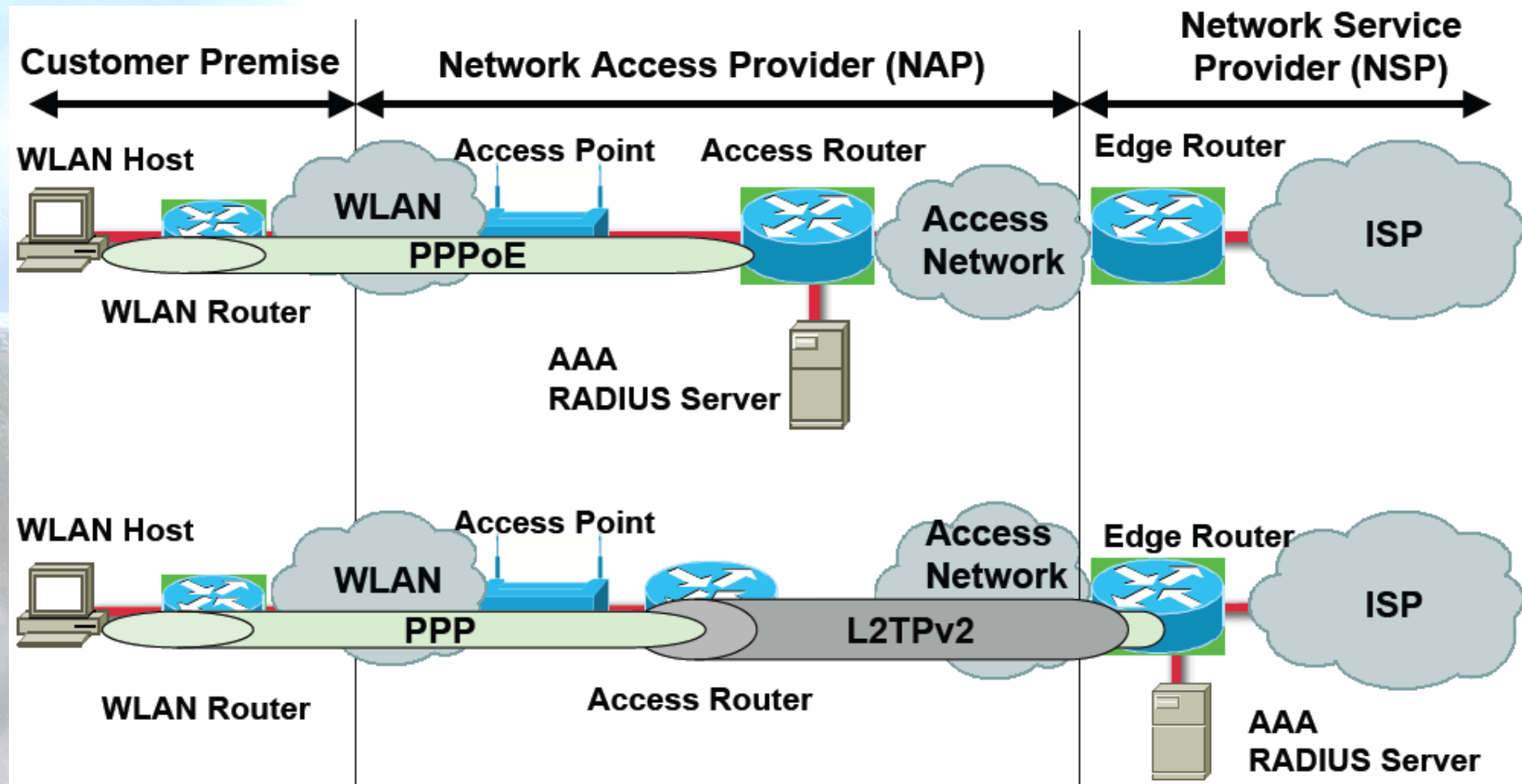


2.2.5 IPv6 in Wireless networks

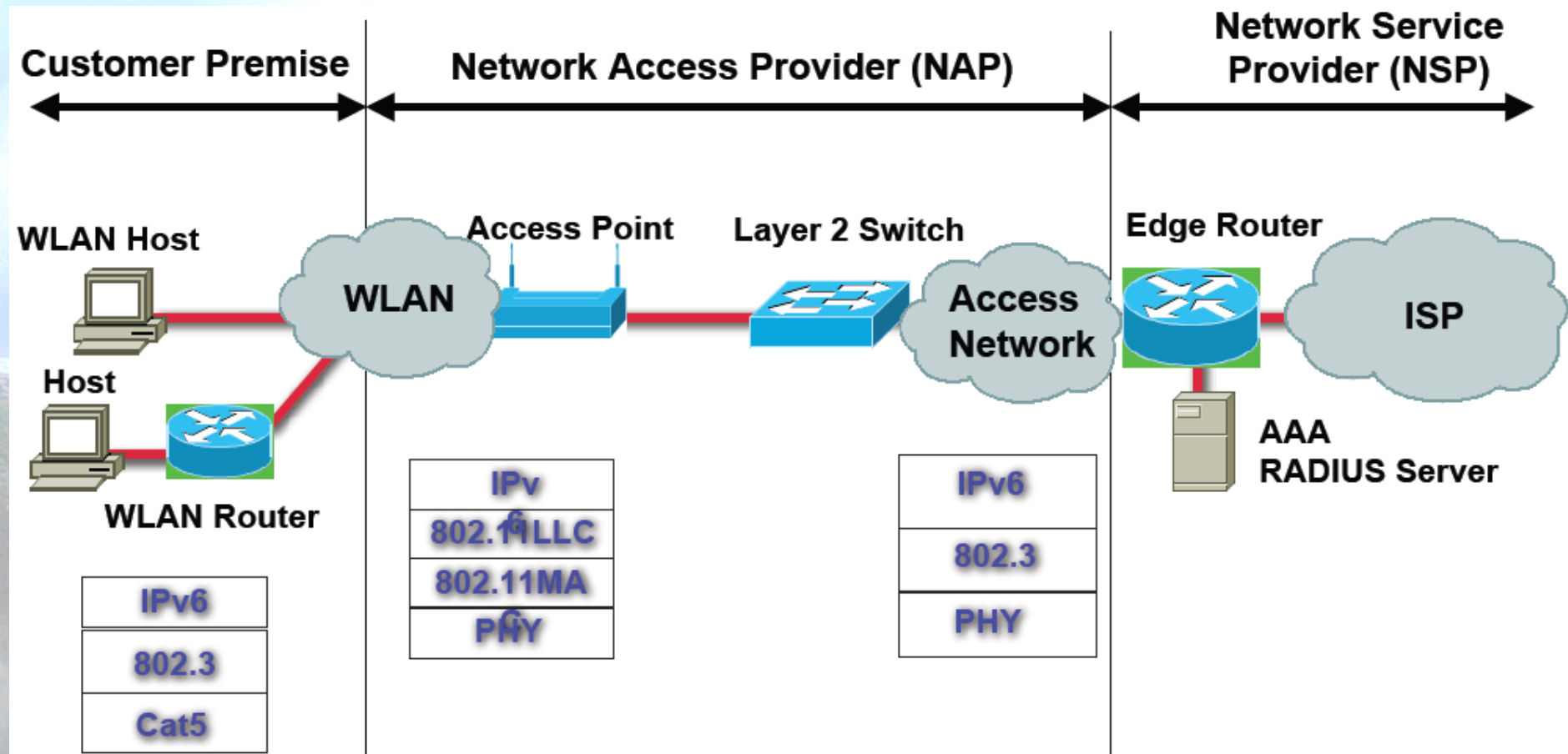
IPv6 Models in wireless networks (1)



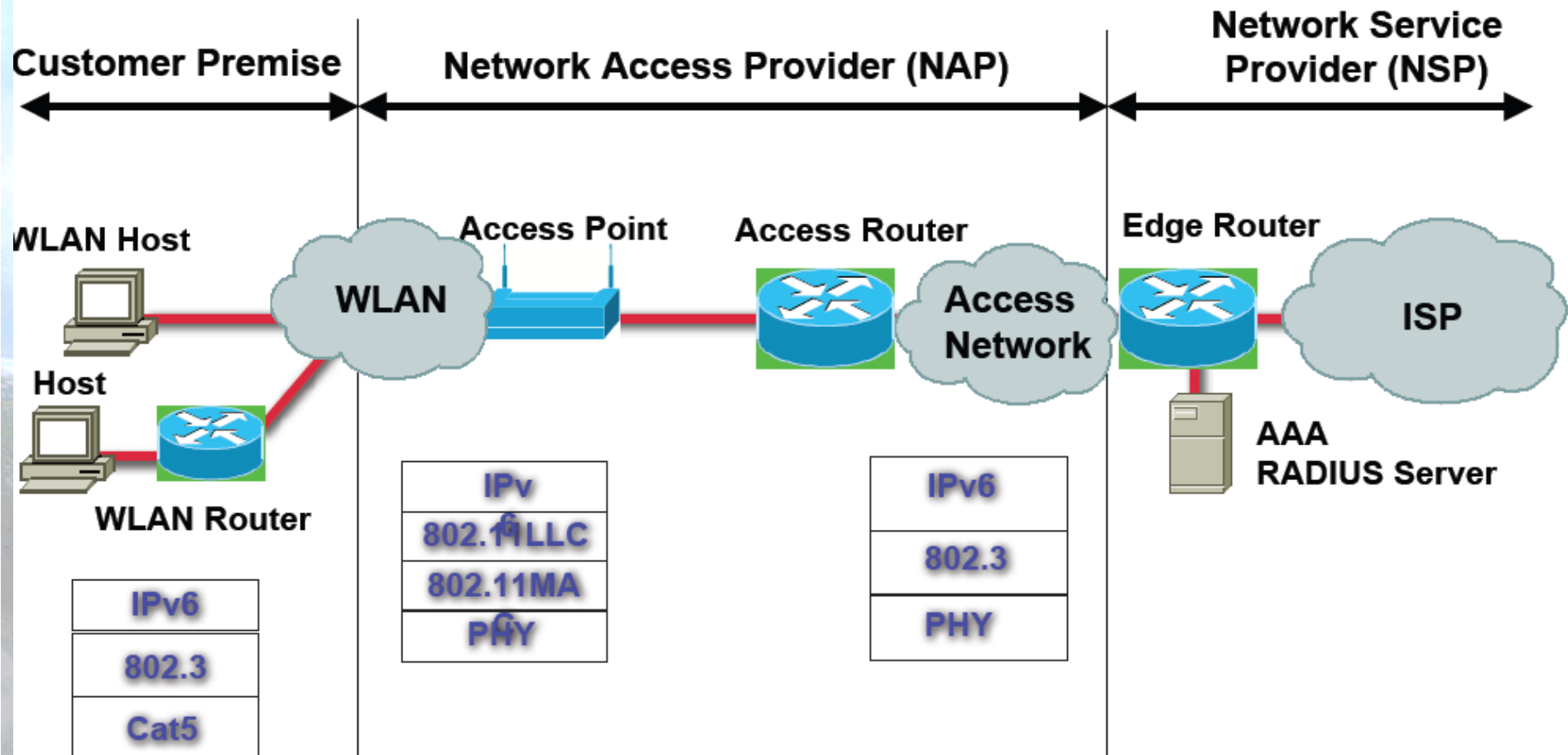
IPv6 Models in wireless networks (2)



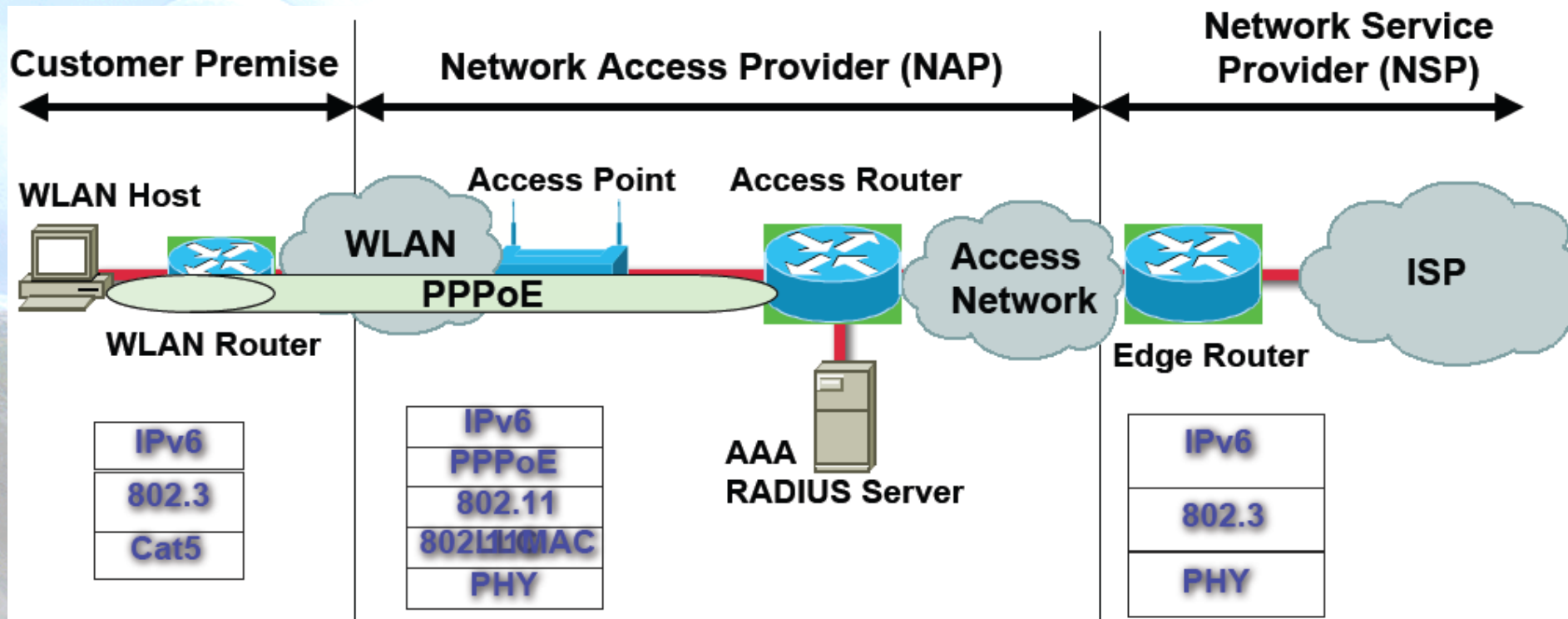
Level 2 Switch between AP & ER



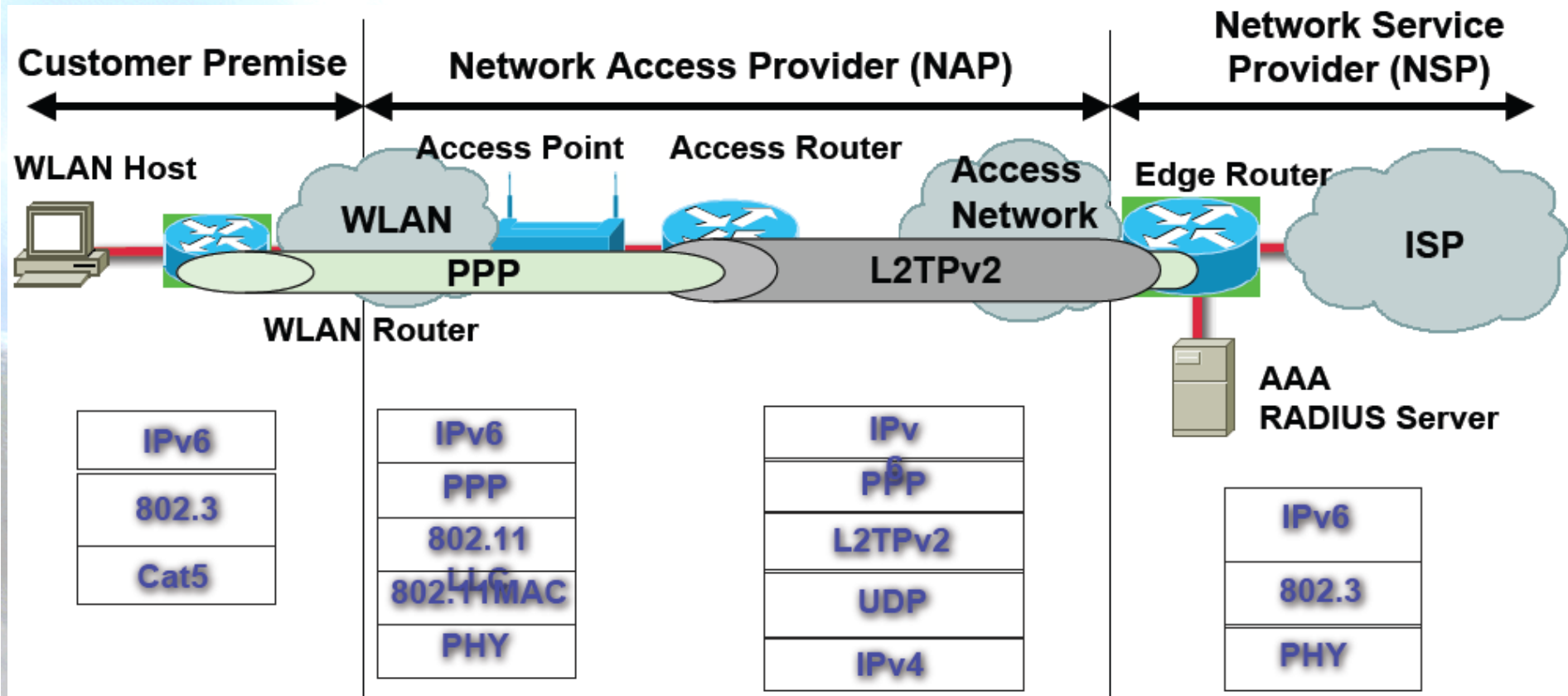
Access Router between AP & ER



PPP Terminated Aggregation (PTA)



L2TPv2 Aggregation (LAA)



References

- EC IST 6LINK, “IPv6 and Broadband”
<http://www.ipv6tf.org/pdf/ISTClusterbooklet2005.pdf>
- Ahmed, Popoviciu and Palet, “IPv6 Deployment Scenarios in Broadband Access Networks”, Barcelona Global IPv6 Summit, June 2005
- Atkinson, Correa and Hedlund, “Explaining International Broadband Leadership,” ITIF May 2008, <http://www.itif.org/index.php?id=142>

IPv6 in broadband access networks

- RFC4779: ISP IPv6 Deployment Scenarios in Broadband Access Networks
 - Describes with detail the deployment of IPv6 in broadband service provider networks
 - Scenarios
 - Integration methods
 - Coexistence with existing IPv4 services
 - Native and tunneling methods

IPv6 in IEEE 802.16 – WiMAX

- RFC4968: Analysis of IPv6 Link Models for IEEE 802.16 Based Networks
- RFC5120: Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks
- RFC5154: IP over IEEE 802.16 Problem Statement and Goals
- RFC5181: IPv6 Deployment Scenarios in 802.16 Networks
 - Describe the model, transmission, deployment scenarios and objectives of IPv6 in IEEE 802.16 networks

IPv6 in 3G

- RFC3314: Recommendations for IPv6 in Third Generation Partnership Project (3GPP) Standards
- RFC3316: Internet Protocol Version 6 (IPv6) for Some Second and Third Generation Cellular Hosts
- RFC3481: TCP over Second (2.5G) and Third (3G) Generation Wireless Networks
- RFC3574: Transition Scenarios for 3GPP Networks
- RFC4083: Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP)
- RFC4215: Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks
- 3GPP Release 5
 - Describe IPv6 peculiarities in 3G networks

Thanks !!

Contact:

– Jordi Palet (Consulintel): jordi.palet@consulintel.es

The IPv6 Portal:

<http://www.ipv6tf.org>

