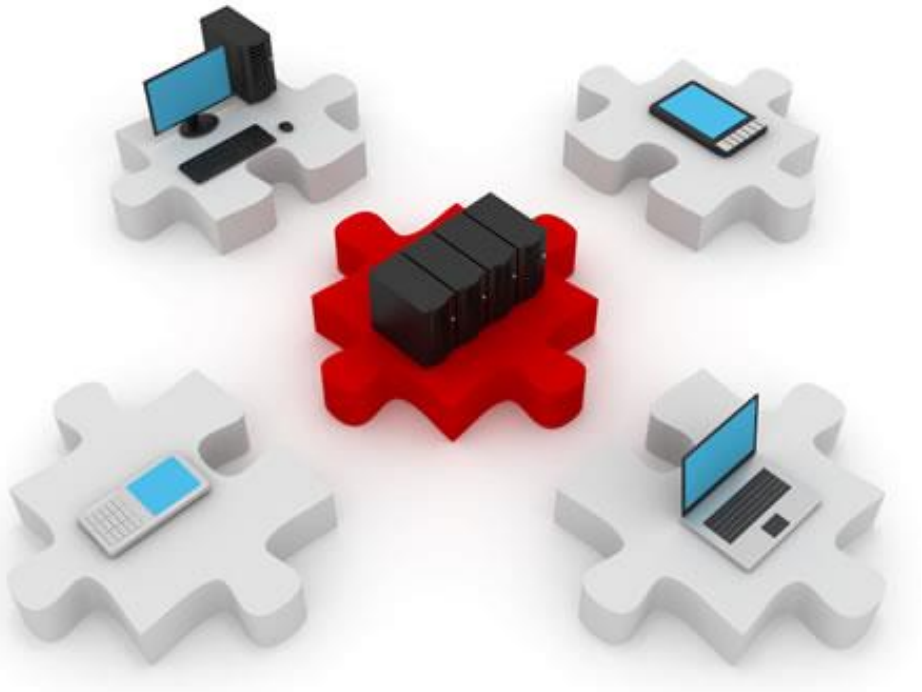
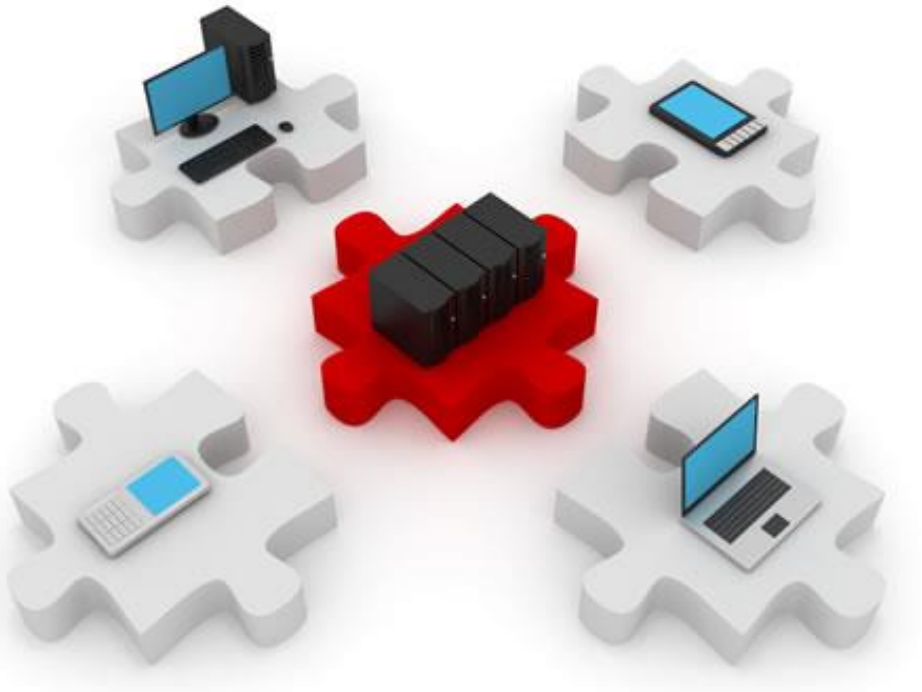


Configuring MPLS VPN & Remote Access

06-ian-2015

What this lecture is about:

- Quick recap of MPLS and MPLS VPN.
- MPLS VPN configuration.
- Cable technologies.
- DSL technologies.



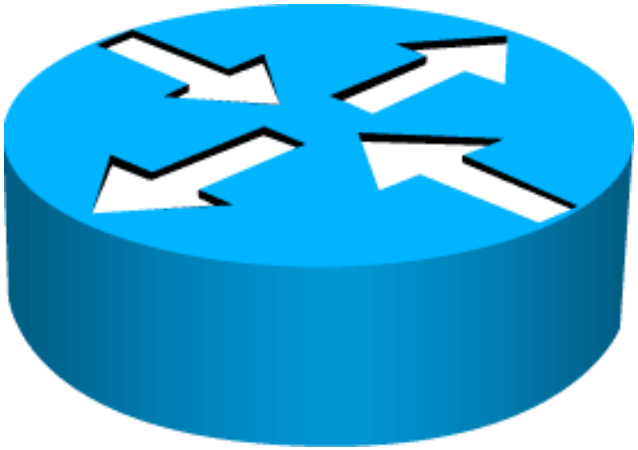
MPLS VPN Reminder

First, a brief recap

Reminder: router types

- With MPLS, we're talking about ISPs and their customers
  - Customers are considered sites (companies) with their own private network.
  - The SP's role is to ensure connectivity between these sites

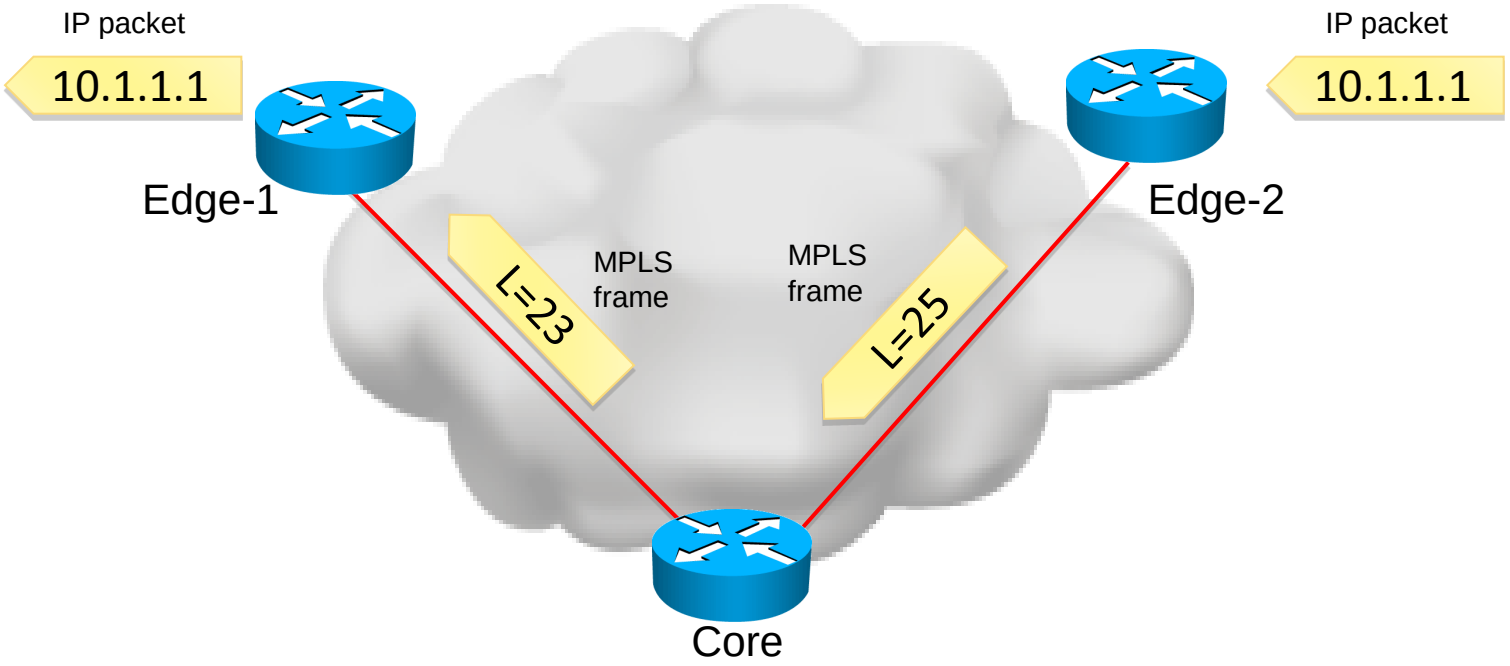
- C (Customer Router)
  - Belongs to a customer's internal network
- CE (Customer Edge Router)
  - Connects to the SP's network
- PE (Provider Edge Router)
  - Connects to customers' network
- P (Provider Router)
  - Internal SP router



Reminder: MPLS features

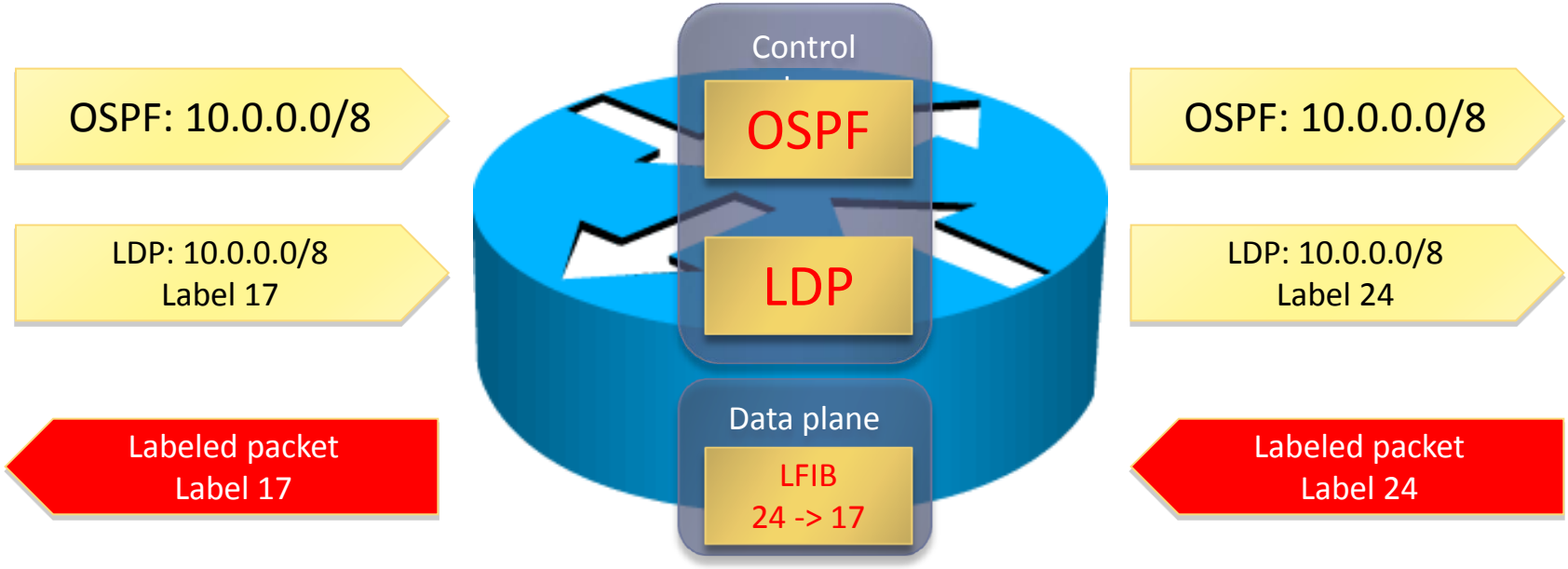
- MPLS reduces routing lookups.
  - MPLS relies on CEF
- MPLS forwards packets based on labels.
  - Label-switching does not involve the routing table
- Labels usually correspond to IP destination networks (equal to traditional IP forwarding).
- Labels can also correspond to other parameters:
  - Layer 3 VPN destination
  - Layer 2 circuit
  - Outgoing interface on the egress router
  - QoS
  - Source address
- Currently, MPLS only supports IPv4.
  - But label switching can work regardless of the L3 protocol

Reminder: MPLS Operation



- Only edge routers must perform a routing lookup.
- Core routers switch packets based on simple label lookups and swap labels.
  - No recursive lookups required.
- How do routers know which label to use?
  - Find out later in this lecture.

Reminder: MPLS components

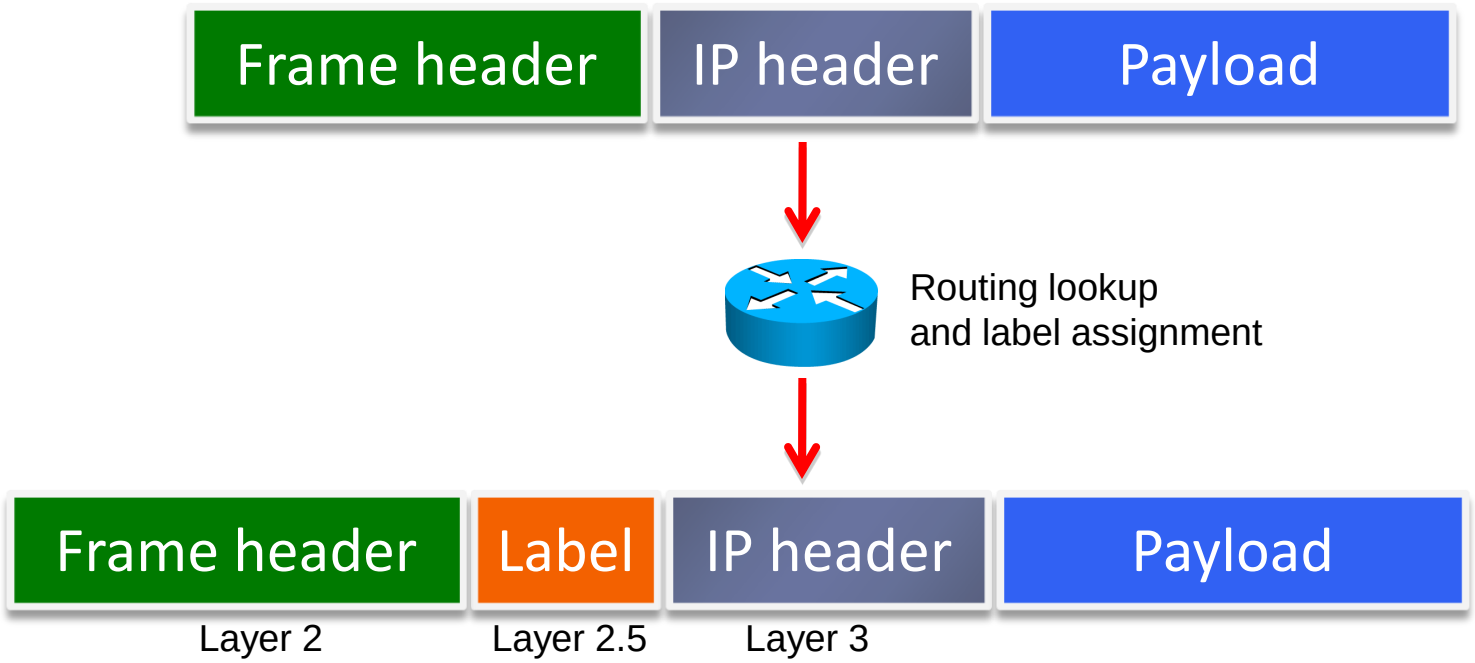


- A Layer3 routing protocol is required to propagate routing information.
- A label exchange mechanism is required to propagate labels for all Layer 3 destinations.
- Information from control plane is sent to the data plane.

Reminder: Label Format

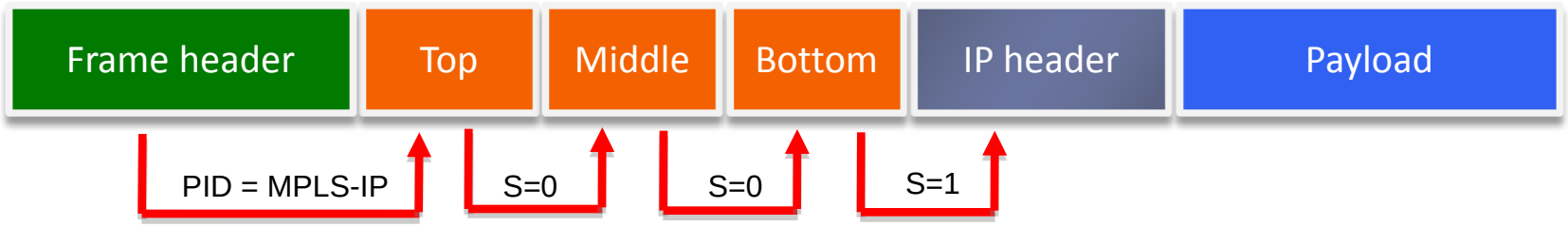
Field	Description
20-bit label	The actual label. Values 0 to 15 are reserved.
3-bit experimental (EXP) field	Used by Cisco to define a class of service (CoS) in order to assign a value for QoS.
1-bit bottom-of-stack indicator	MPLS allows multiple labels to be inserted. The bottom-of-stack bit determines if this label is the last label in the packet. If this bit is set (1), the setting indicates that this label is the last label.
8-bit Time to Live (TTL) field	Has the same purpose as the TTL field in the IP header.

Reminder: Where does the label fit into?



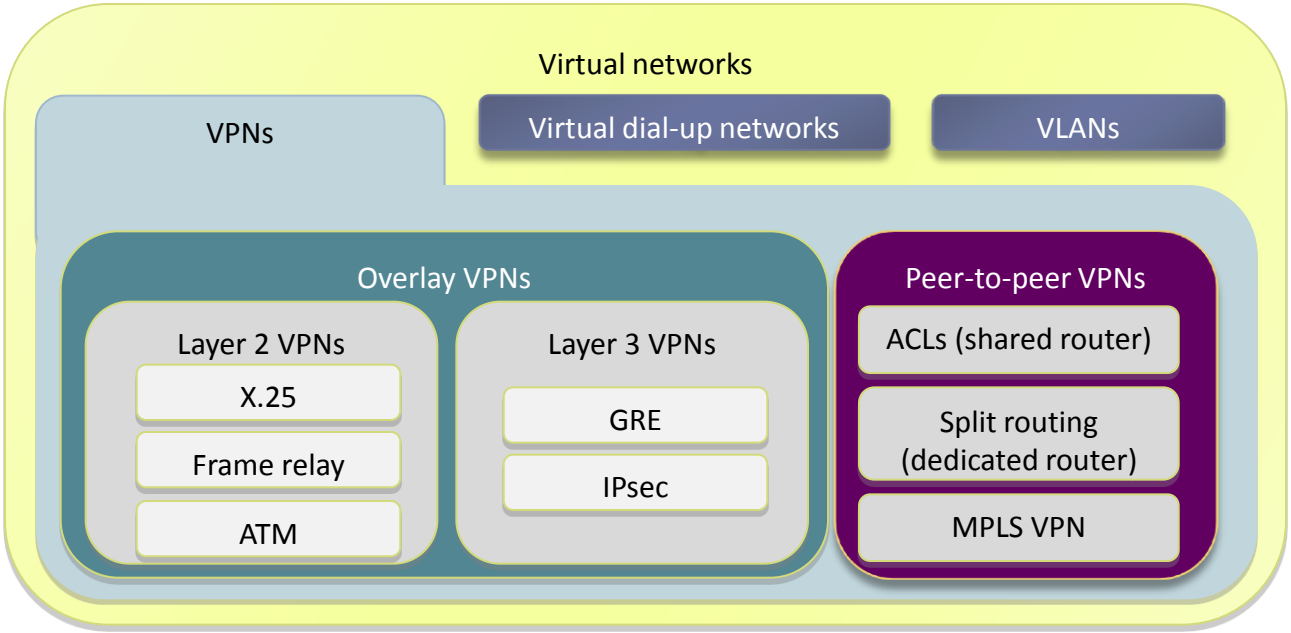
- An MPLS label is announced by the frame's Ethertype field.
- An MPLS label does not store the encapsulated protocol
  - How does an edge LSR that removes the last label what protocol lies inside?

Reminder: Label Stack



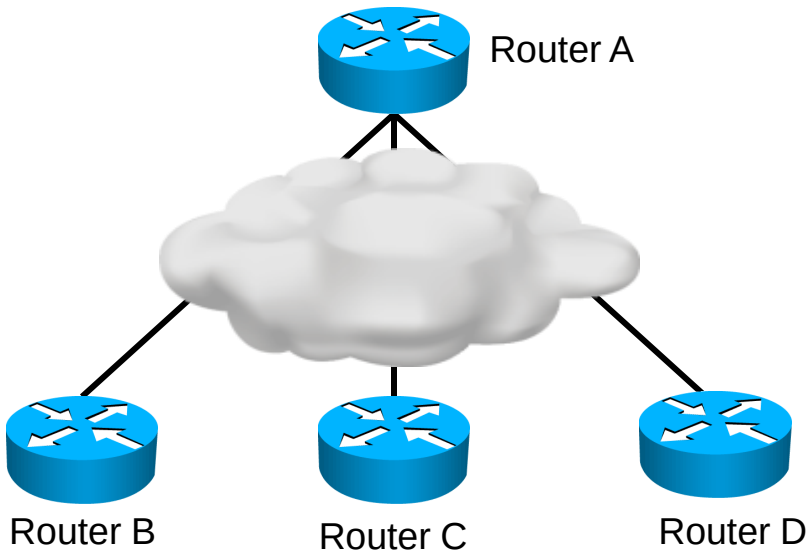
- There may be more than one label in an MPLS packet.
- Only the outermost label is used to route/switch packets in the MPLS domain.
- The bottom-of-stack bit indicates whether the next header is another label or a Layer 3 header.
- Other labels allow services like:
  - MPLS VPNs
  - Traffic engineering (TE)

Reminder: VPN Taxonomy



- There are two types of VPN topologies
  - **Overlay VPNs**: the SP provides virtual point-to-point links
    - Customers send their routes through their own tunnels.
  - **Peer-to-peer VPNs**: the SP participates in customer routing
    - The SP is aware and transports the customers' routes.

Reminder: Layer 3 Overlay VPNs

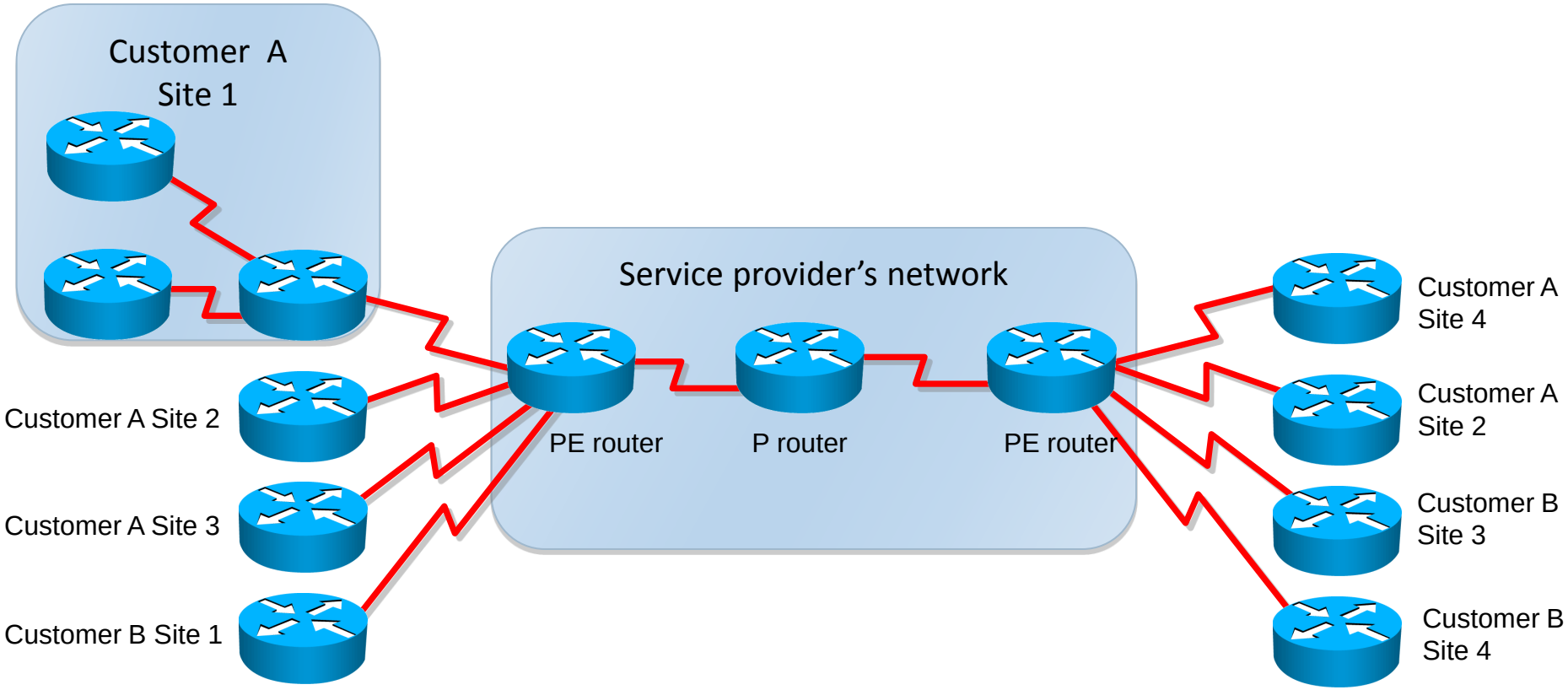


- The service provider infrastructure appears as point-to-point links to customer routes.
- Routing protocols run directly between customer routers.
  - Adjacencies are established over the SP network
- The use of tunnels allows the use of private addresses (RFC 1918).
  - Interconnecting sites with private addressing can be done without NAT

Reminder: Peer-to-peer VPNs

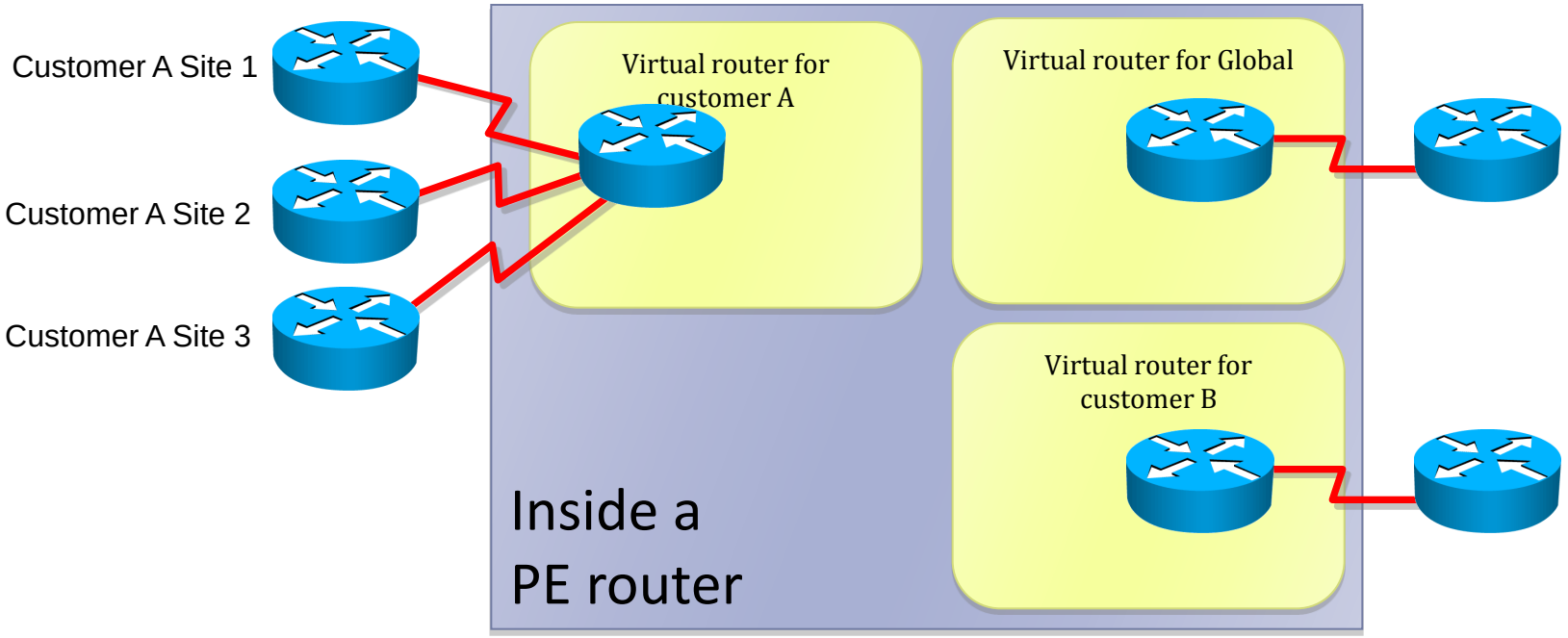
- The SP and the customers use the same network protocol (IPv4, for example).
- The SP's core carries all customer routes
  - PE routers exchange routing information with CE routers
  - CE routers establish L3 adjacencies only with the PE routers
    - This greately reduces the overhead of full or partial mesh topologies
  - PE routers exchange routing information required for sites to communicate.
    - The SP has to run a routing protocol capable of carrying customer routes.
- The SP's network is a public address space
  - But it carries customer routes that are very likely to use private addressing: first problem.

Reminder: Sample MPLS VPN architecture



- PE routers transport customer routes
  - P routers simply provide fast transport, without routing knowledge

Reminder: PE router architecture in MPLS VPN



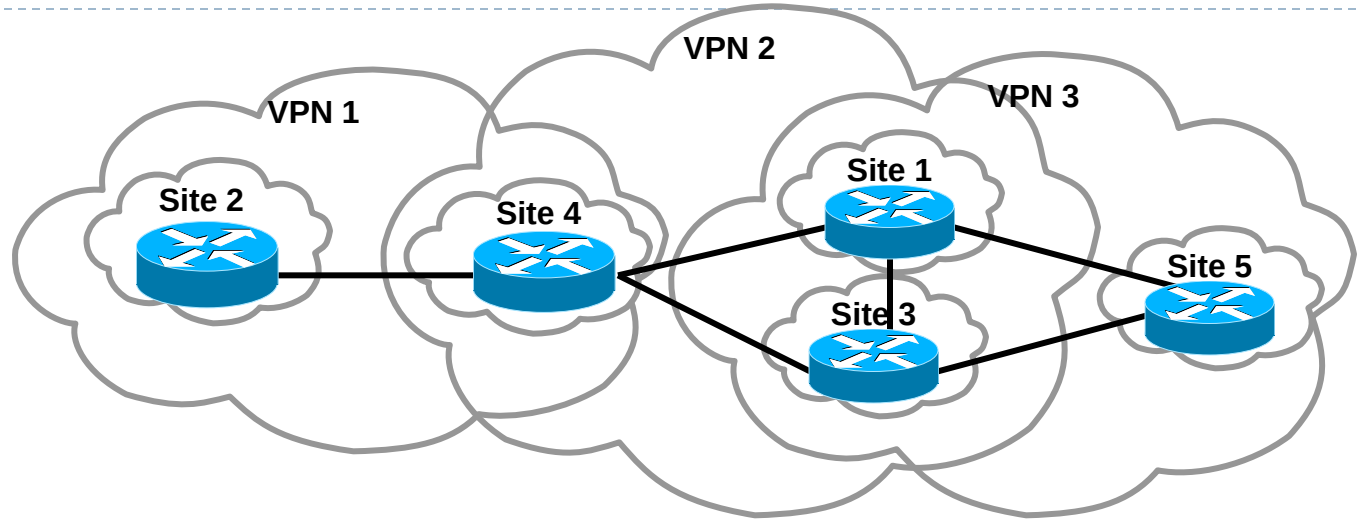
- A PE router is internally divided into multiple virtual routers
  - Each virtual router connects one customer
  - Each customer is assigned an independent **Virtual Routing and Forwarding** (VRF) table
  - Each VRF corresponds to a dedicated PE router in the traditional peer-to-peer model

Reminder: Route Distinguishers

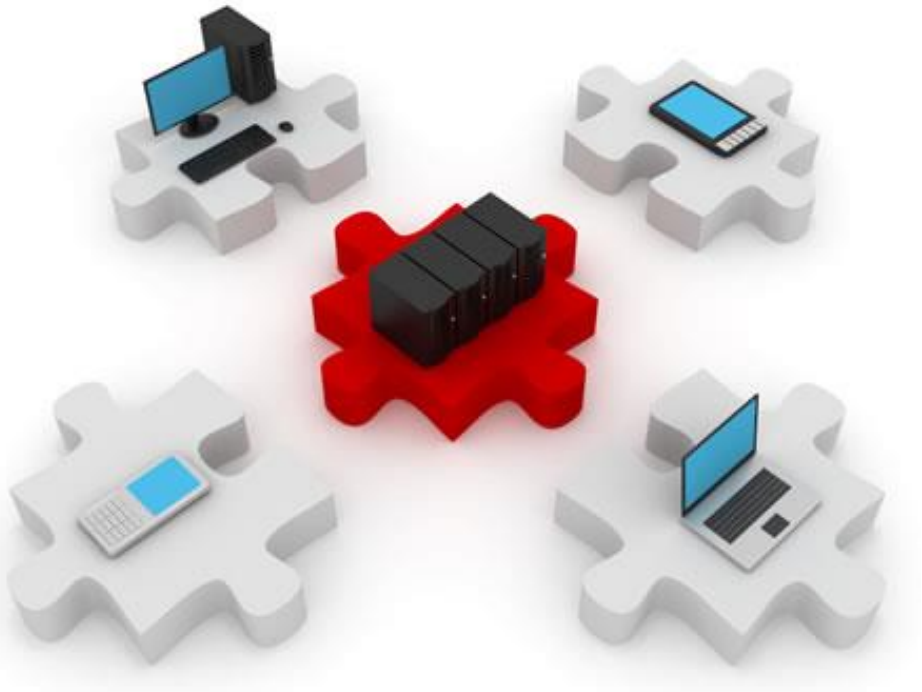
Question?	How is information about overlapping subnets of two customers propagated via a single routing protocol?
Answer:	Extend the customer addresses to make them unique.

- The 8-byte RD is prepended to an IPv4 address to make the address globally unique.
- The resulting address is a VPNv4 address.
- VPNv4 addresses are exchanged between PE routers via BGP.
- BGP that supports address families other than IPv4 addresses is called multiprotocol BGP (MPBGP).

Reminder: Route Targets



- Some sites participate in more than one VPN.
  - For example the VoIP VPN and the inter-site VPN
- The RD only identifies routes from the same customer
  - But if the customer participates in more than one VPN, all its routes will have the same RD.
- RTs were introduced in the MPLS VPN architecture to support complex VPN topologies.
- RTs are additional attributes that attach to VPNv4 BGP routes to indicate VPN membership.



Configuring MPLS VPN

Configuring the VRF

- Consider the VRF to be a small router dedicated to one customer only.
- The VRF must have a name, a unique route distinguisher, and must specify which routes will be imported and exported for this customer.
- For one client:

```
PE1(config)#ip vrf MY_FIRST_VRF
PE1(config-vrf)#rd 999:1
PE1(config-vrf)#route-target import 999:1
PE1(config-vrf)#route-target export 999:1
PE1(config-vrf)#exit
PE1(config)#
```

- The route target value is independent of the route distinguisher's value.
- The notation 999:1 stands for 2 bytes represented by 999, followed by 6 bytes that end in 1.

Configuring multiple VRFs

- Route targets allow certain VRFs to receive routes from other customers, too:

```
PE1(config)#ip vrf MY_FIRST_VRF
PE1(config-vrf)#rd 999:1
PE1(config-vrf)#route-target import 999:1
PE1(config-vrf)#route-target export 999:1

PE1(config)#ip vrf MY_SECOND_VRF
PE1(config-vrf)#rd 999:2
PE1(config-vrf)#route-target both 999:2
PE1(config-vrf)#route-target import 999:1
```

- The second VRF will allow its customer to communicate its routes securely but also to receive routes from the other VRF/client.

Filtering routes with route maps

- For finer tuning, a route map can be used to filter only specific routes (the route map has to be created, of course):

```
PE1(config)# route-map CUSTOMER_IMPORT_MAP permit 10
PE1(config-route-map)#match ip address ?
  <1-199>       IP access-list number
  <1300-2699>   IP access-list number (expanded range)
  WORD          IP access-list name
  prefix-list   Match entries of prefix-lists
  <cr>

PE1(config-vrf)# import map CUSTOMER_IMPORT_MAP
```

- Basic “permit” statements in the ACLs indicate routes that will be allowed.

VRFs and interfaces

- A VRF must also be assigned to an interface to indicate to the router where the customer is located:

```
PE2(config)# interface FastEthernet0/0
PE2(config-if)# ip vrf forwarding MY_FIRST_VRF
```

- Make sure you configure the VRF before applying the IP address on the interfac, otherwise you will see something like this:

```
% Interface FastEthernet0/0 IP address 11.100.1.2 removed
due to enabling VRF MY_FIRST_VRF
```

- You can still apply the IP address on the interface afterwards.
- One VRF can be associated with multiple interfaces.

BGP configuration

- BGP must be configured to carry VPNv4 routes.
- First, neighbor relationships must be established between BGP-speaking routers (mainly PE routers):

```
Router(config)# router bgp 999
Router(config-router)# no synchronization
Router(config-router)# no bgp default ipv4-unicast
Router(config-router)# neighbor 180.17.1.8 remote-as 999
Router(config-router)# neighbor 180.17.1.8 update-source loopback0
Router(config-router)# neighbor 180.17.1.9 remote-as 999
Router(config-router)# neighbor 180.17.1.9 update-source loopback0
```

AS Number

Deactivate ordinary BGP operation

- Next, BGP must do two other things:
  - Redisitribute the customer's IPv4 routes in BGP
  - Send those routes as VPNv4 routes in the Extended Community attribute of BGP.

IPv4 and VPNv4

- We'll define two address families: for IPv4 and VPNv4 routes.

- First, the IPv4 address family:

```
PE1(config-router)# address-family ipv4 vrf MY_FIRST_VRF
PE1(config-router-af)# redistribute rip metric 1
PE1(config-router-af)# exit-address-family
```

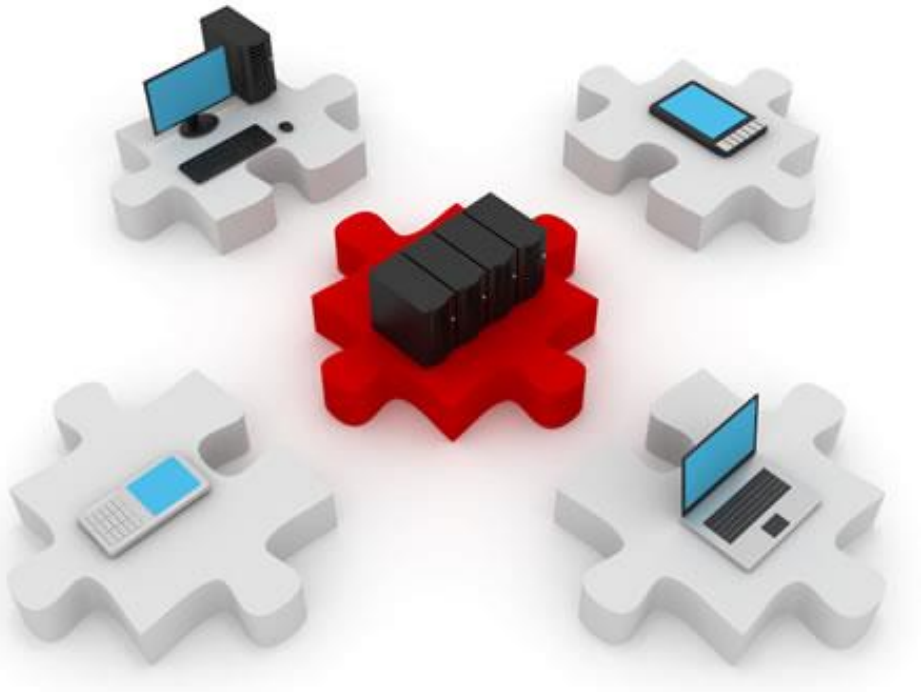
- Then, the VPNv4 address family:

```
PE1(config-router)# address-family vpnv4
PE1(config-router-af)# neighbor 180.17.1.8 activate
PE1(config-router-af)# neighbor 180.17.1.8 send-community
extended
PE1(config-router-af)# exit-address-family
```

Customer's routing protocol

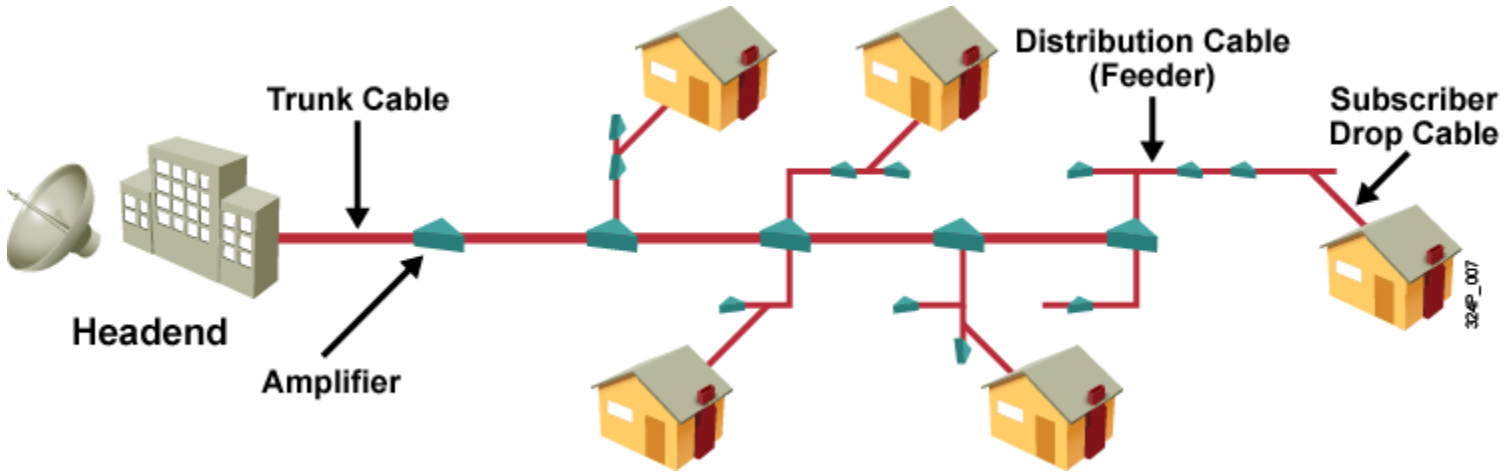
- Finally, all we have to do is to run the same routing protocol as our customer.
  - For redistribution to work, both routing protocols must be running on the same router.
- Route redistribution occurs now from BGP into the customer's routing protocol.
  - But only routes imported in this VRF will be redistributed, not all BGP routes.

```
PE1(config)# router rip
PE1(config-router)# version 2
PE1(config-router)# address-family ipv4 vrf MY_FIRST_VRF
PE1(config-router-af)#redistribute bgp 64512 metric 1
PE1(config-router-af)# network 10.0.0.0
PE1(config-router-af)# no auto-summary
PE1(config-router-af)# version 2
PE1(config-router-af)# exit-address-family
```



Cable Technologies

What is a cable system?



- CATV originally meant “community antenna television.” This form of transmission shared TV signals.
- Cable systems were originally built to extend the reach of TV signals and improve over-the-air TV reception.
- Modern cable systems use fiber and coaxial cable for signal transmission.
- Modern cable systems provide two-way communication between subscribers and the cable operator:
  - High speed Internet access
  - High definition TV
  - Residential phone lines

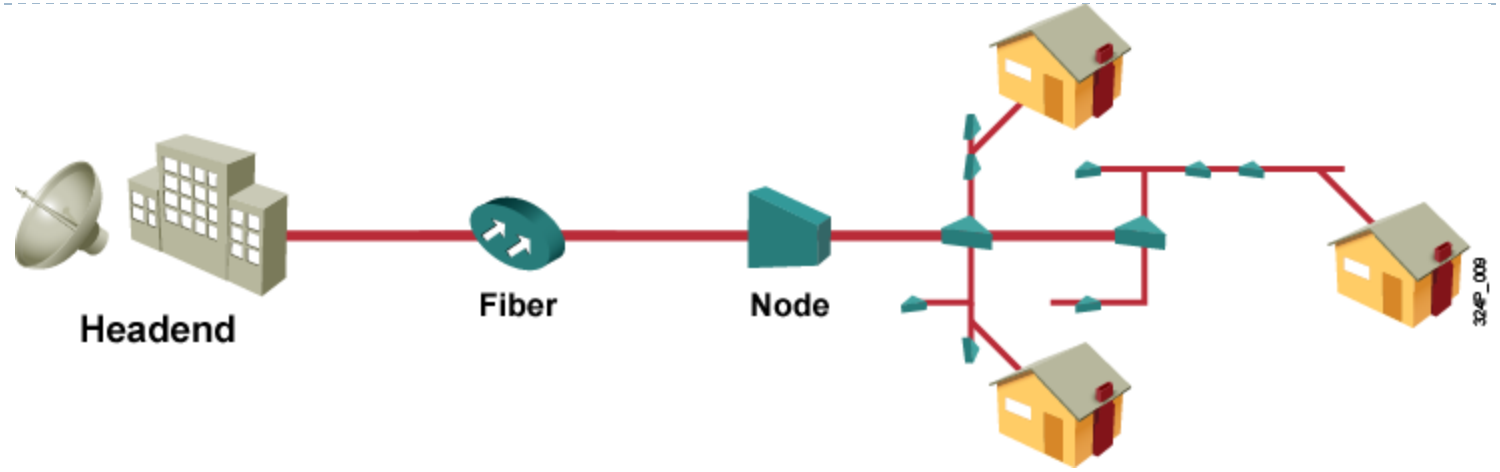
Cable technology terms

- Broadband
  - Frequency division multiplexing (FDM) of many signals over the same wide radio frequency (RF) bandwidth
- CATV
  - Modern residential cable systems
- Coaxial cable
  - Signal attenuates over distance.
  - Attenuation causes bad TV reception and slow data transfers.
- Tap
  - Divider for an RF signal, used to connect multiple subscribers.

Cable tehnology terms

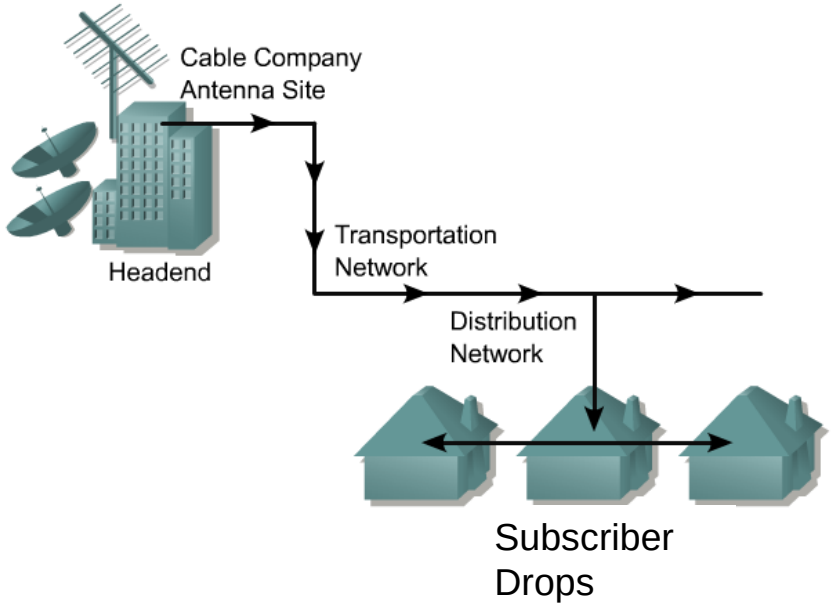
- Amplifier
  - Used to increase distance of signal; noise is also amplified.
- HFC
  - Hybrid Fiber and Coaxial network that uses optical fiber to replace the trunk portion of the network.
  - Coaxial cable is still used for subscriber connections.
- Downstream
  - Signal flow from the headend to the subscribers.
- Upstream
  - Signal flow from the subscribers to the headend.

HFC architecture



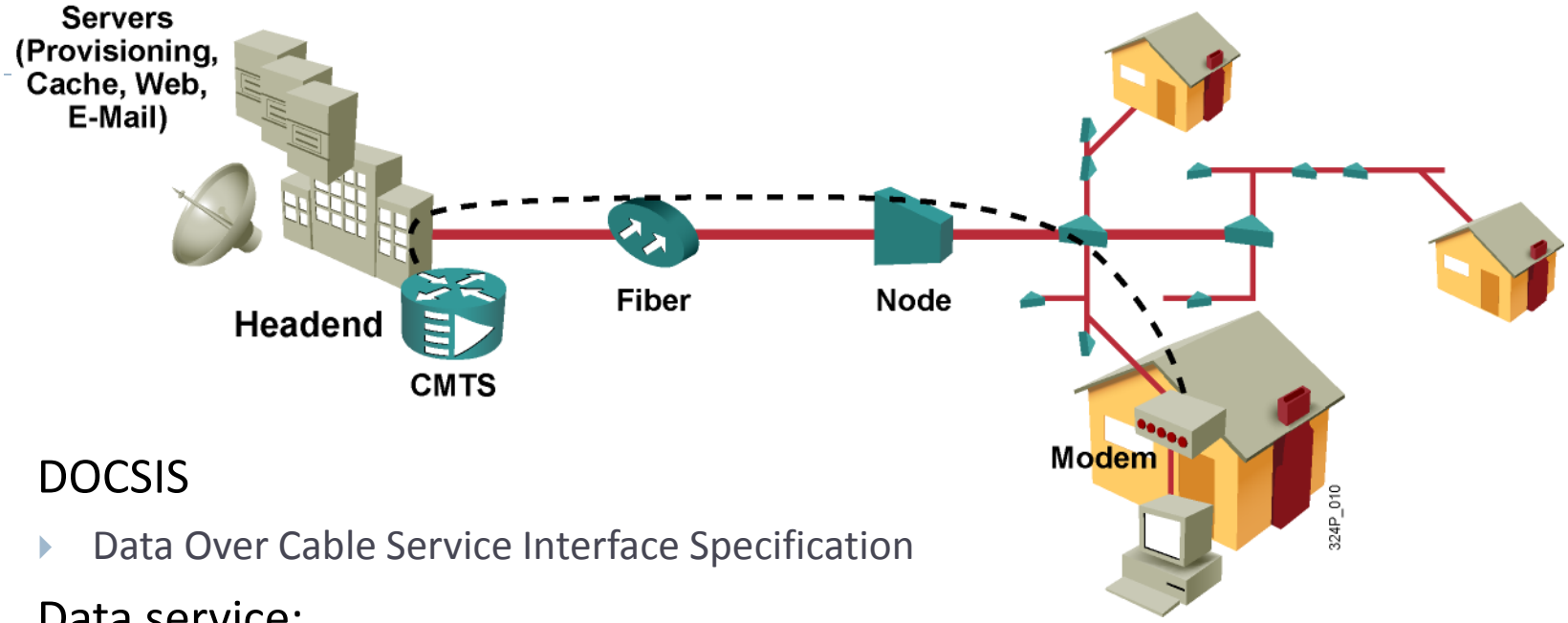
- Using fiber provides many benefits:
  - Reduces the use of amplifiers
  - Is thin and lightweight
  - Covers long distances
  - Solves the noise problem
  - Immune to external interference

Cable system components



- Antenna site
  - Satellite reception site.
- Headend
  - Main facility for signal processing.
- Transportation network
  - Single backbone used to reach long distances and distribution networks.
- Distribution network
  - “Tree-and-branch”: backbone that connects many subscribers.
- Subscriber drop
  - Cable segment that reaches the customer premises.

Sending data over cable

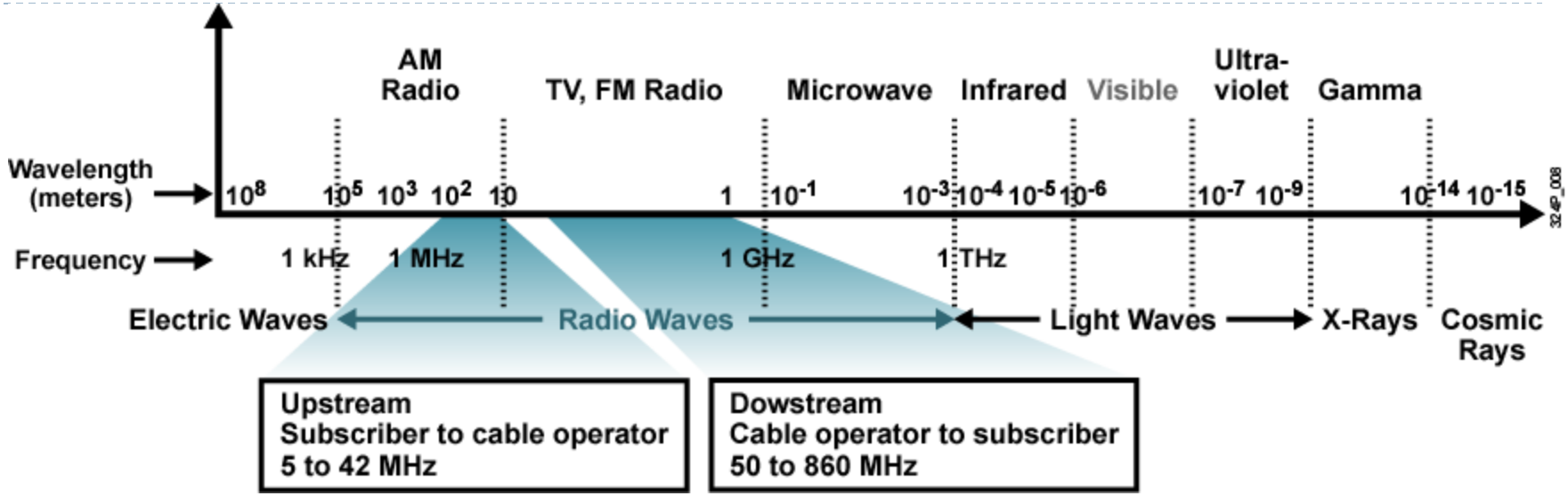


- DOCSIS
  - Data Over Cable Service Interface Specification
- Data service:
  - runs between cable modem (CM) and cable modem termination system (CMTS).
- Users on a segment share upstream and downstream bandwidth.
- Bandwidth can reach 27 Mbps downstream and 2.5 Mbps upstream.
- Up to 2000 subscribers can be connected to the same network segment.
- Subscribers cannot directly communicate with each other because the CM's upstream frequency is different from its downstream frequency.

Cable system benefits

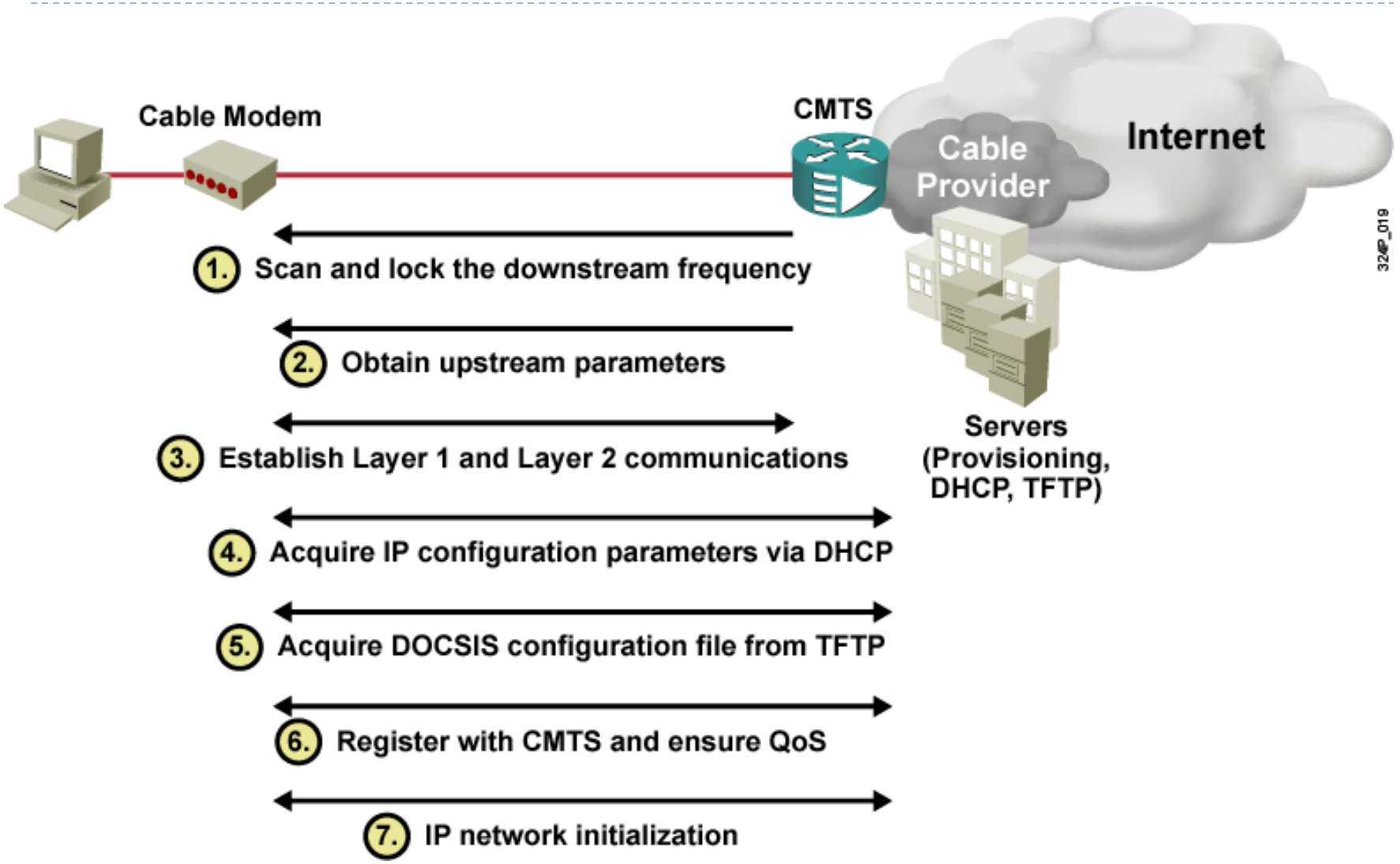
- Cable is cost-effective because it combines many services over the same infrastructure.
- Cable supports different services:
  - Analog video
  - Digital video
  - Voice
  - Data
    - File transfer
    - Video/audio streaming and VoIP
    - VPN connectivity
- Inexpensive high-speed Internet access enables the application of advanced SOHO and teleworker deployments.

Digital signals over radio waves



- Cable uses a part of RF electromagnetic frequencies.
- Cable can transmit signals in either direction.
- RF portion used is subdivided into channels for:
  - Downstream: Headend-to-subscriber has 810 MHz of RF bandwidth.
  - Upstream: Subscriber-to-headend has 37 MHz of RF bandwidth.

Provisioning a cable modem



Provisioning a cable modem

- **Downstream setup:** The CM powers up and then scans and locks the downstream path for the appropriate RF.
- **Upstream setup:** The CM listens to the management messages received through the downstream path. The messages include information on how, where, and when to communicate in the upstream path.
- **Layers 1 and 2 establishment:** The CM communicates with CMTS to establish physical and data link layer parameters.
- **Obtaining an IP address:** The CM requests IP configuration parameter information (IP address, default gateway, and TFTP server) from the DHCP server.

Provisioning a cable modem

- **Getting the DOCSIS configuration:** The CM requests a DOCSIS configuration file from the TFTP server. A DOCSIS configuration file is an ASCII file and includes settings, such as downstream channel identification, class of service (CoS) settings, baseline privacy settings, general operational settings, network management information, and vendor-specific settings.

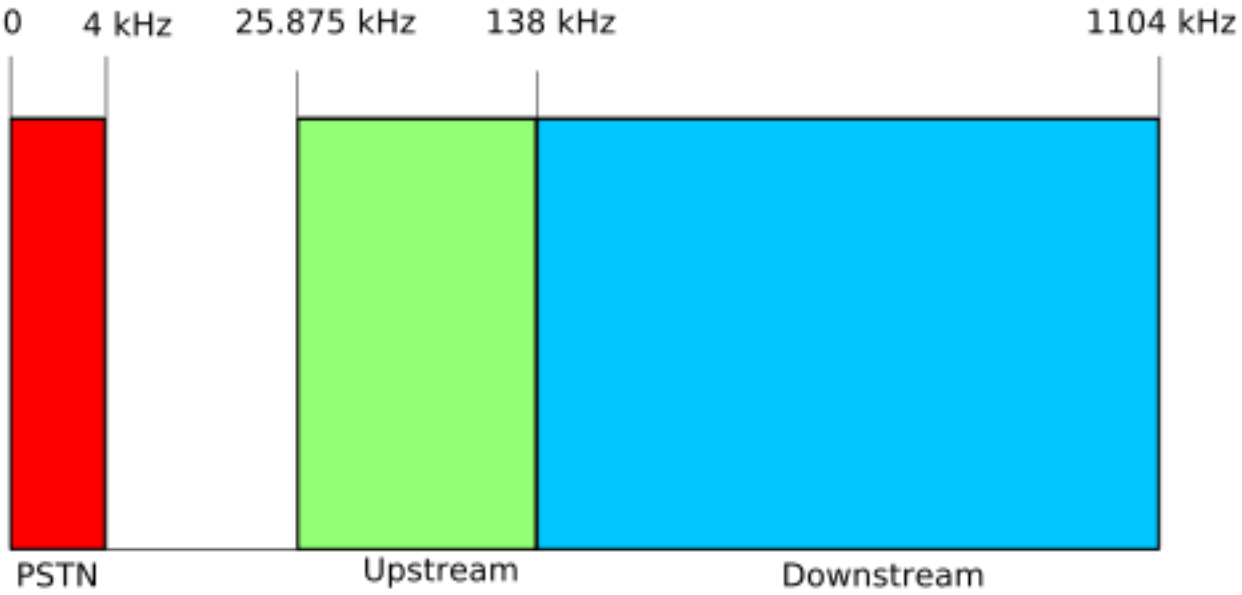
- **Register QoS with CMTS:** The CM registers, negotiates, and ensures QoS settings with the CMTS.

- **IP network initialization:** That is, the PC requests its own IP configuration parameters from the DHCP server. If multiple PC connections behind the CM are required, a router can be used.

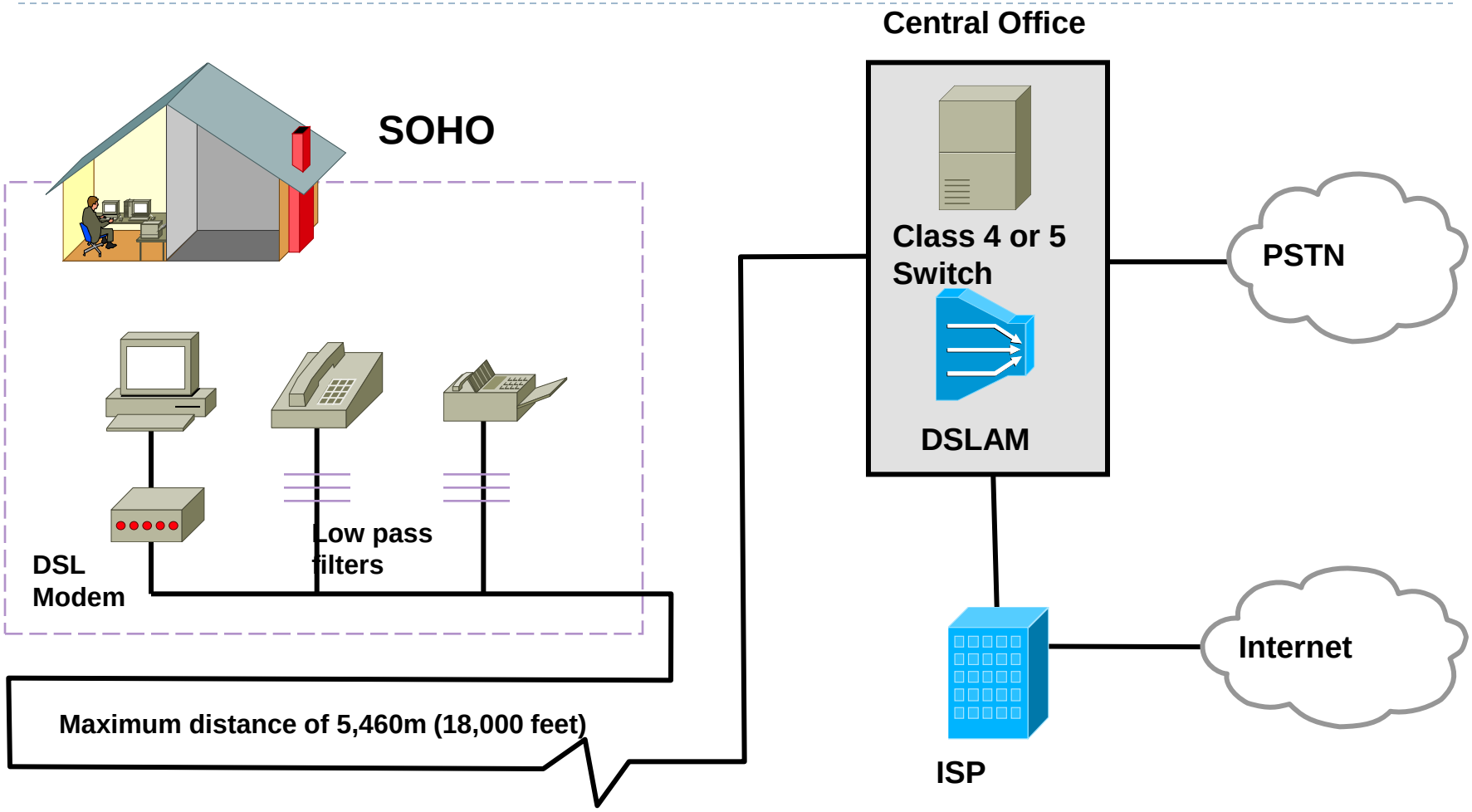
DSL Technologies

DSL = Digital Subscriber Line

- For many years, the telephone networks did not use the bandwidth above 3 kHz.
- Advances in technology allowed DSL to use the additional bandwidth from 3 kHz up to 1 MHz to deliver high-speed data services over ordinary copper lines.



Typical DSL Topology



- DSL modems are required to connect to a DSLAM (DSL Access Multiplexer)

Types of DSL

- **Symmetrical DSL:** Upstream and downstream speeds are the same.
- **Asymmetrical DSL:** Upstream and downstream speeds are different. Downstream speed is typically higher than upstream speed.
- The term xDSL covers a number of DSL variations, such as ADSL, high-data-rate DSL (HDSL), Rate Adaptive DSL (RADSL), symmetric DSL (SDSL), ISDN DSL (IDSL), and very-high-data-rate DSL (VDSL).

DSL Technology	Nature	Max. Data Rate (Down / Up) [bps]	Data and POTS
ADSL	Asymmetric	8 M / 1 M	Yes
VDSL	Symmetric or Asymmetric	52 M / 13 M	Yes
IDSL	Symmetric	144 k / 144 k	No
SDSL	Symmetric	768 k / 768 k	No
HDSL	Symmetric	2 M / 2 M	No
G.SHDSL	Symmetric	2.3 M / 2.3 M	No

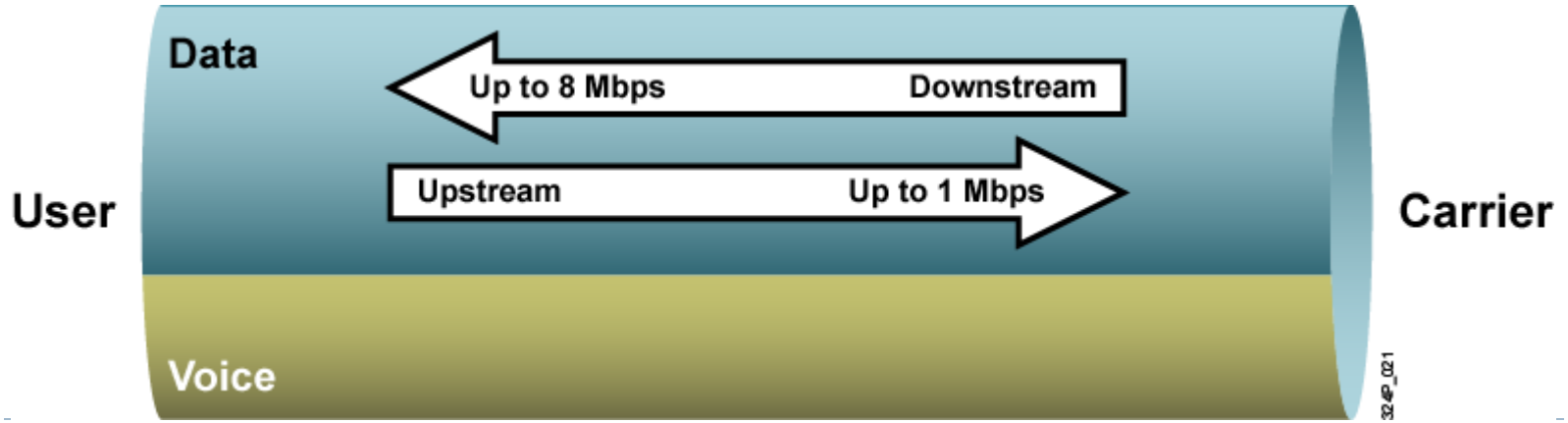
DSL distance limitations

DSL Technology	Max. Data Rate (Down / Up) [bps]	Max. Distance [feet / km]
ADSL	8 M / 1 M	18,000 / 5.5
VDSL	52 M / 13 M	4,500 / 1.4
IDSL	144 k / 144 k	18,000 / 5.5
SDSL	768 k / 768 k	22,000 / 6.7
G.SHDSL	2.3 M / 2.3 M	28,000 / 8.5

- Maximum data rate and distance assume ideal conditions.
- Maximum data rate is achieved at shortest distance.
- Maximum distance is achieved at lowest data rate.

ADSL

- ADSL is the most common implemented DSL technology today.
  - And also one of the most widespread SOHO broadband Internet access technologies.
- ADSL coexists with POTS on the same wire
  - Filters are used to separate the signals
- A greater bandwidth portion is assigned to the downstream path.
  - End users typically need to download more than to upload.
- 8 Mbps download and 1 Mbps upload; up to 5.5 Km from the carrier's office. But not both at the same time… ☺



ADSL Speed vs Distance

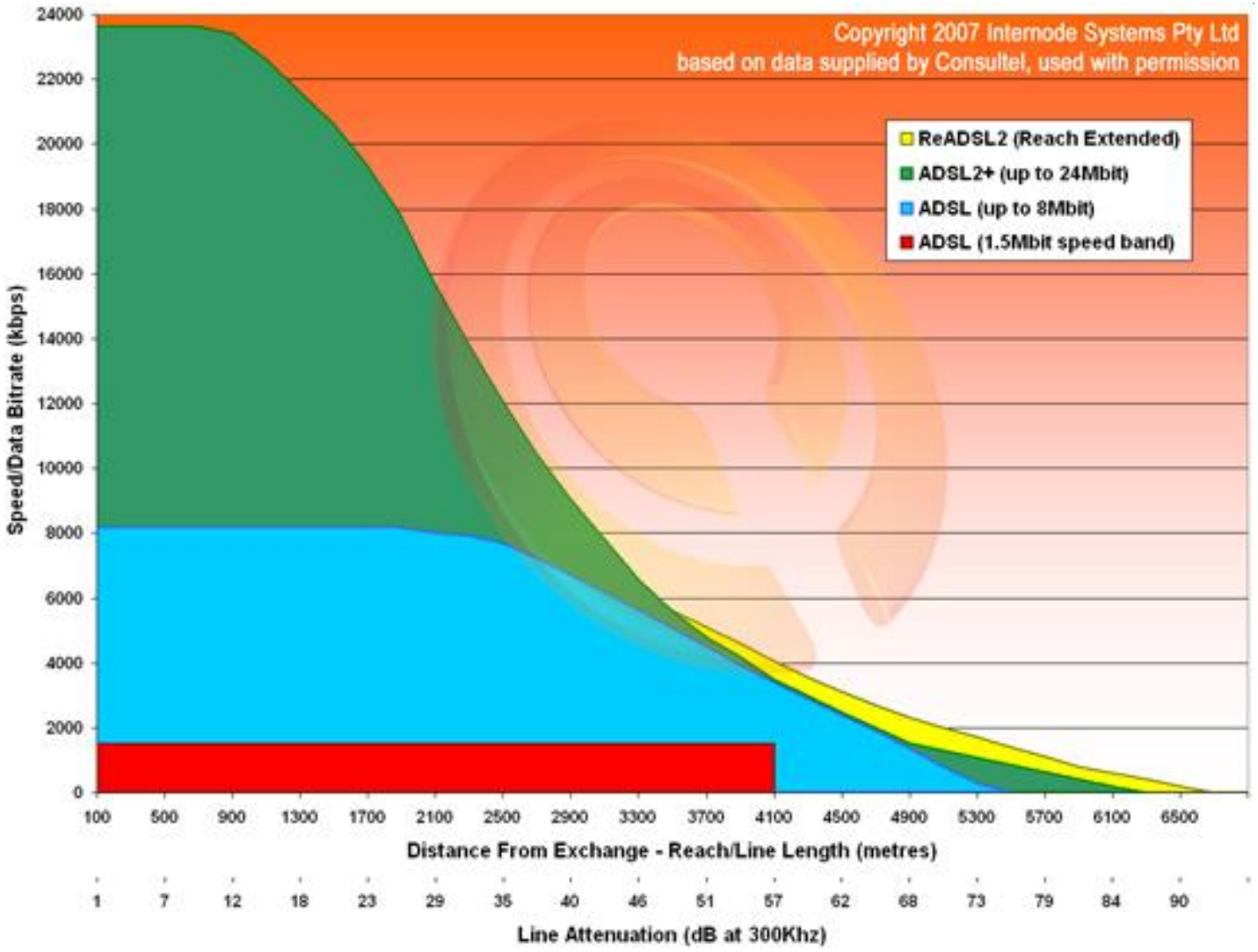
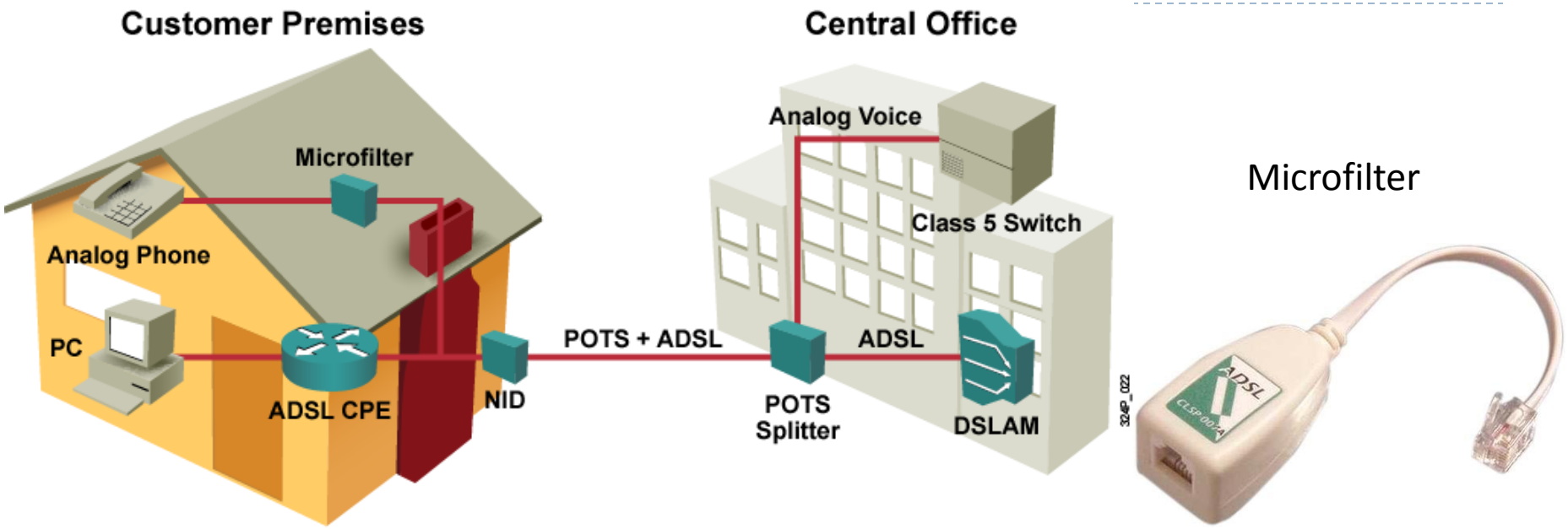


Image source: http://www.internode.on.net/residential/adsl_broadband/easy_broadband/performance/

Splitters

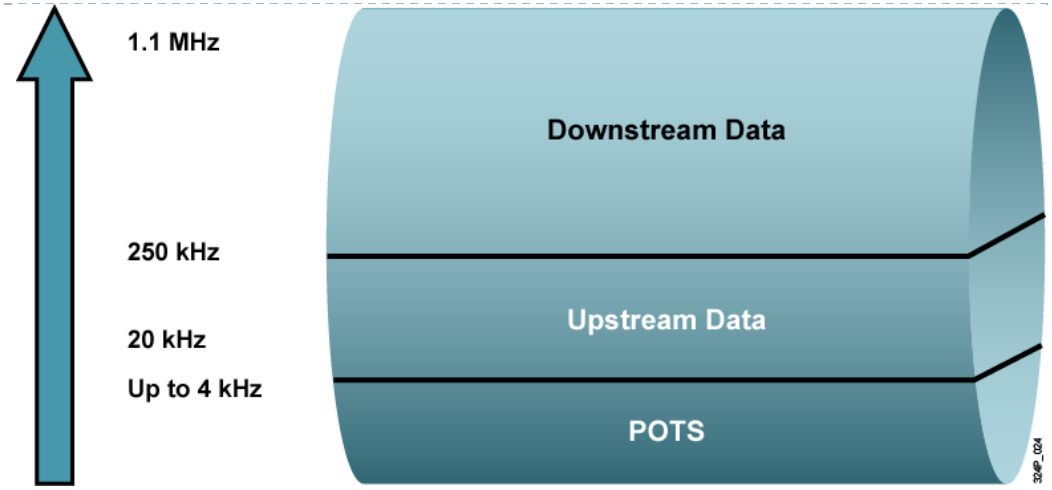


- A key feature of ADSL is coexistence with POTS.
- Transmission of voice and data signals is performed on the same wire pair.
- Data circuits are offloaded from the voice switch and terminated by a DSLAM.
- The customer can use a microfilter to remove the ADSL signal from the wire before plugging it into a phone.

ADSL characteristics

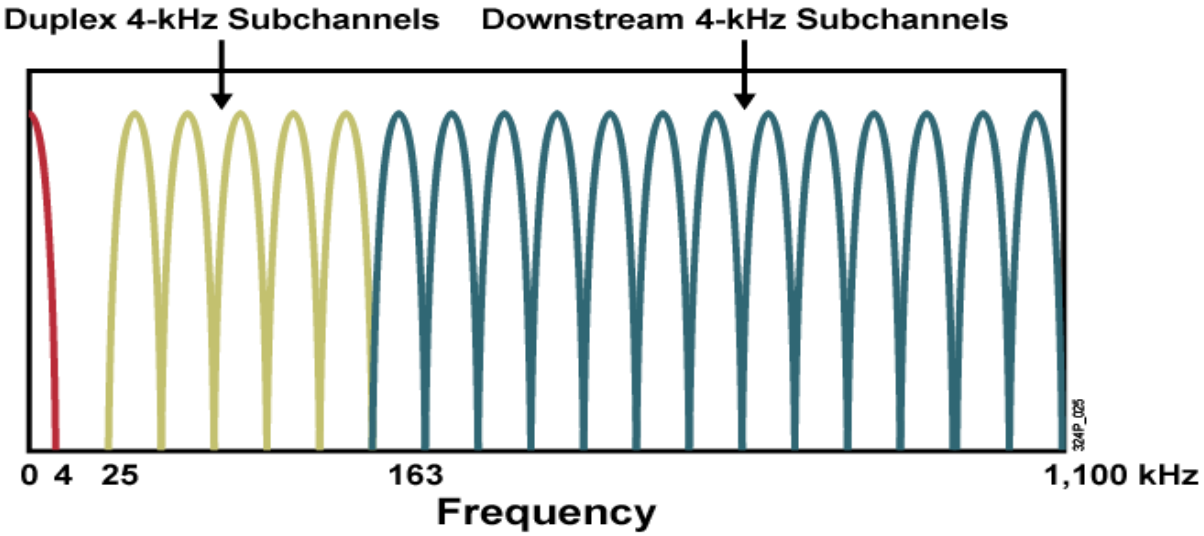
- ADSL equipment:
  - ADSL terminal unit-remote (ATU-R)
  - DSLAM encompassing many ADSL terminal unit-central office (ATU-C)
- ADSL features three basic line-coding techniques:
  - Single carrier—CAP modulation
  - Multicarrier with DMT
  - Multicarrier with G.lite
- ADSL operation and performance are influenced by different impairments.
  - Crosstalk
  - EM noise

ADSL CAP modulation



- A single carrier signal is used.
- The signal is divided into three distinct bands:
  - Voice channel, between 0 and 4 Khz
  - Upstream channel, between 25 and 160 Khz
  - Downstream channel, between 240 Khz and 1.1 Mhz
- Buffer regions are maintained between channel to minimize interference.

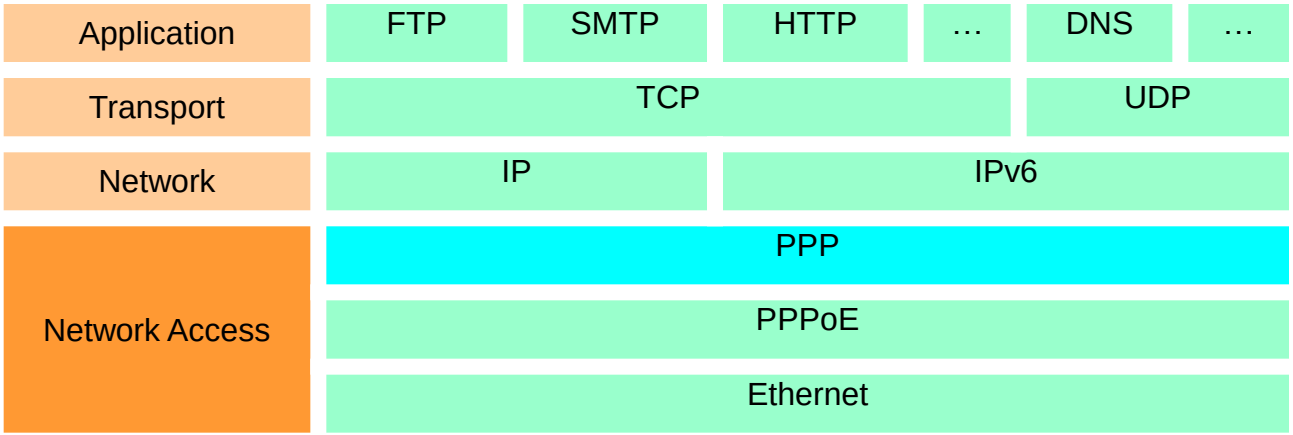
ADSL DMT modulation



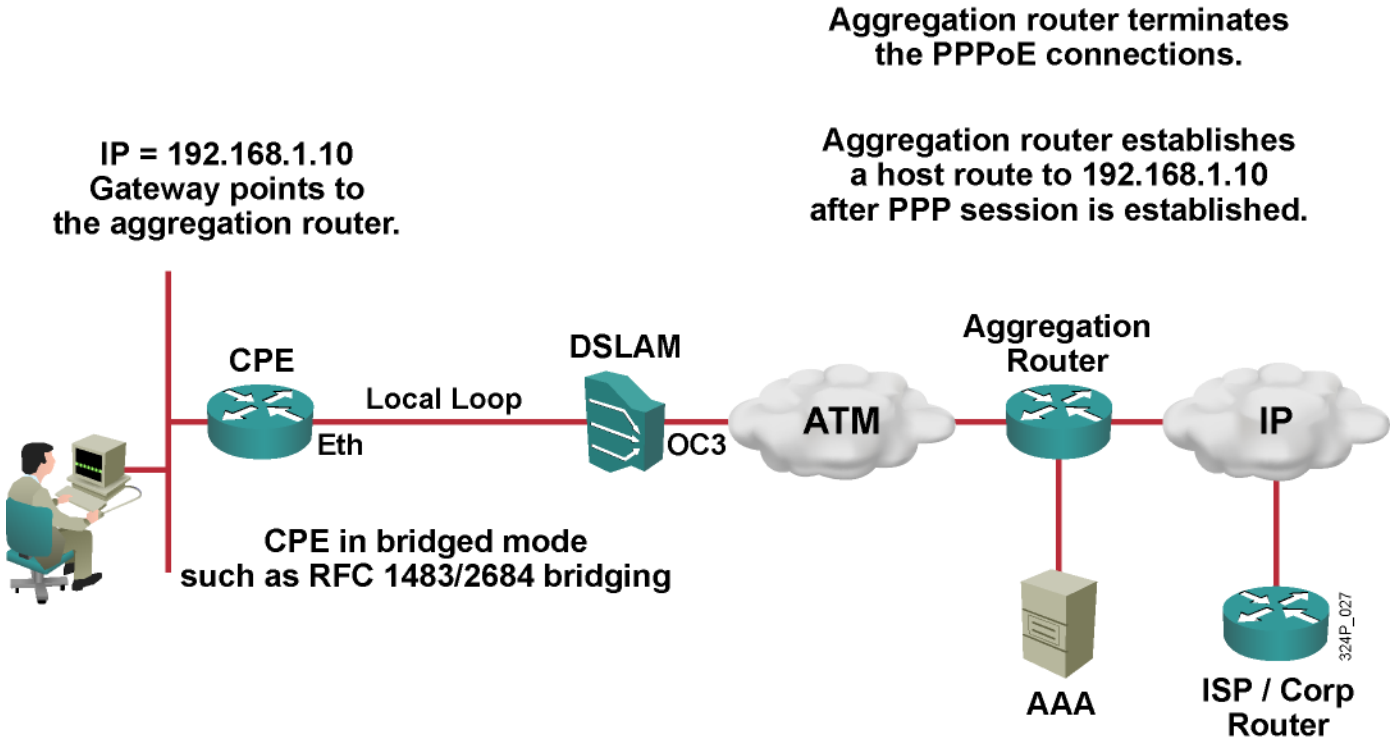
- DMT divides the frequency band into 256 separate 4 kHz-wide channels.
- Channels 6 to 38 are duplex and used for both upstream and downstream data traffic.
- To compensate for noise, the system constantly monitors each channel.
  - When channel quality decreases, the system adjusts the number of bits per channel.
  - If the quality is too impaired, the signal shifts to another channel.

PPP over Ethernet

- An Ethernet frame carries the PPP frame.
- Service provider end:
  - DSLAM for DSL connection termination
  - Aggregation router for PPP session termination
- Subscriber end:
  - DSL modem for DSL connection termination
  - PPPoE client for PPP session termination
- The client device is the PC or the router at the CPE.

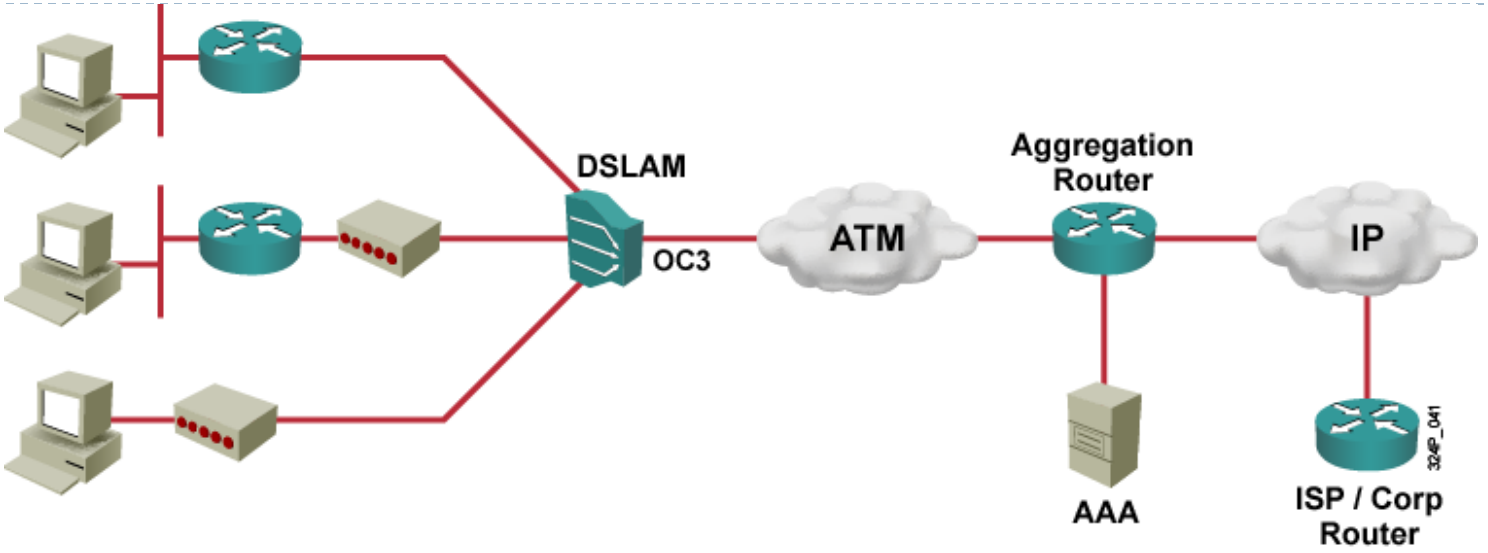


PPPoE in operation



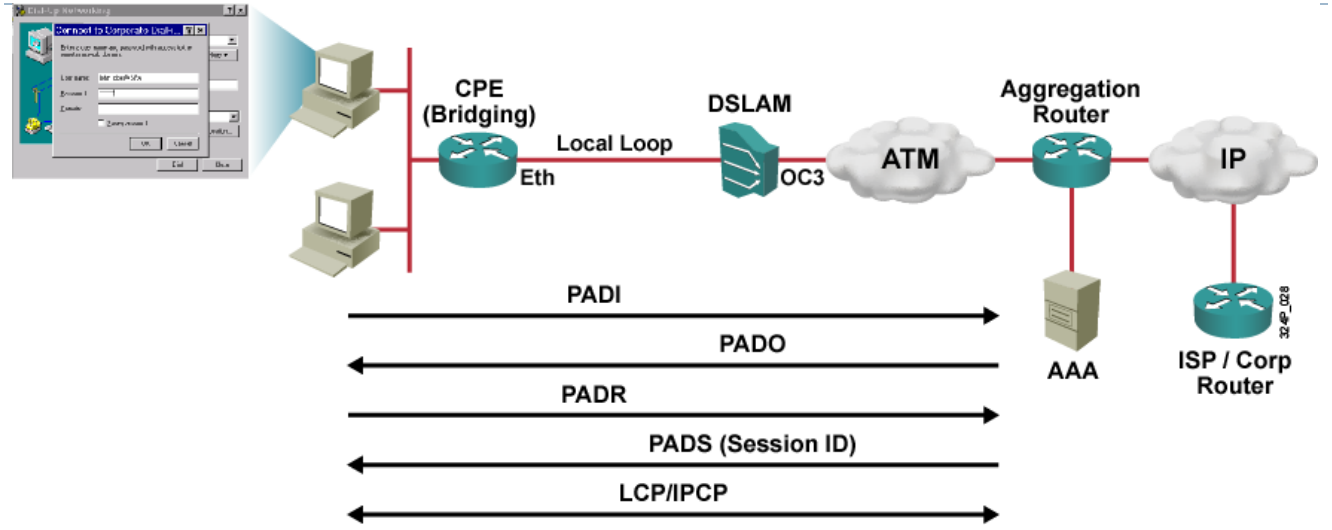
- IP is assigned to PPPoE client functioning device.
- A CPE router can connect multiple users via a single ADSL connection using NAT/PAT and DHCP.

DSL and PPPoe deployment options



- DSL and PPPoE deployment types:
  - Router terminating DSL and with PPPoE client
  - Modem terminating DSL and router with PPPoE client
  - Modem terminating DSL and end-user PC with PPPoE client

PPPoE session establishment



- The PPPoE client broadcasts a PPPoE Active Discovery Initiation (PADI) packet, requesting service.
- The aggregation router sends a PPPoE Active Discovery Offer (PADO) packet, describing provided services.
- The client sends a PPPoE Active Discovery Request (PADR).
- The server replies with a PPPoE Active Discovery Session-confirmation (PADS) confirmation message.

Sooo, WHAT IS security???

Sooo, WHAT IS security???