Cisco Systems

poweredbycisco. networkers 2005

Session AGG-2023

PPOX/L2TP Broadband Aggregation Design and Architectures

Juan Pablo Segura, CCIE 6929

Recuerde siempre:

- **Apagar su teléfono móvil/pager, o usar el modo “silencioso”.**

- **Completar la evaluación de esta sesión y entregarla a los asistentes de sala.**

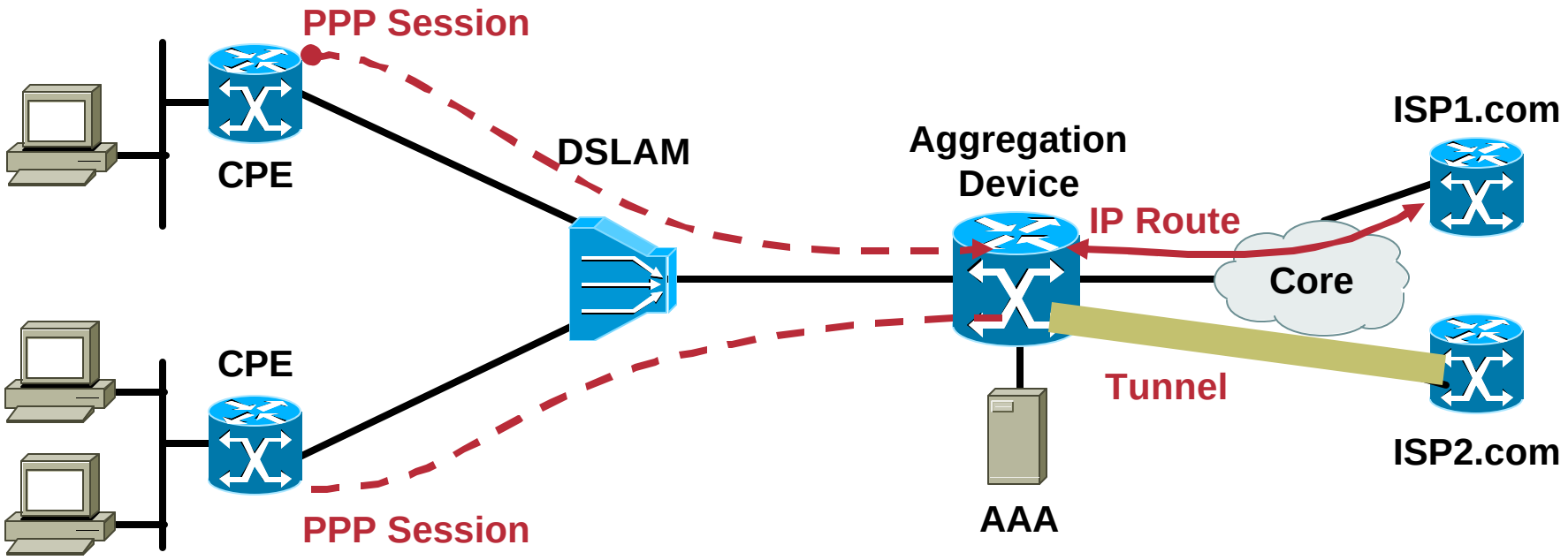
- **Ser puntual para asistir a todas las actividades de entrenamiento, almuerzos y eventos sociales para un desarrollo óptimo de la agenda.**

- **Completar la evaluación general incluida en su mochila y entregarla el miércoles 8 de Junio en los mostradores de registración. Al entregarla recibirá un regalo recordatorio del evento.**

Agenda

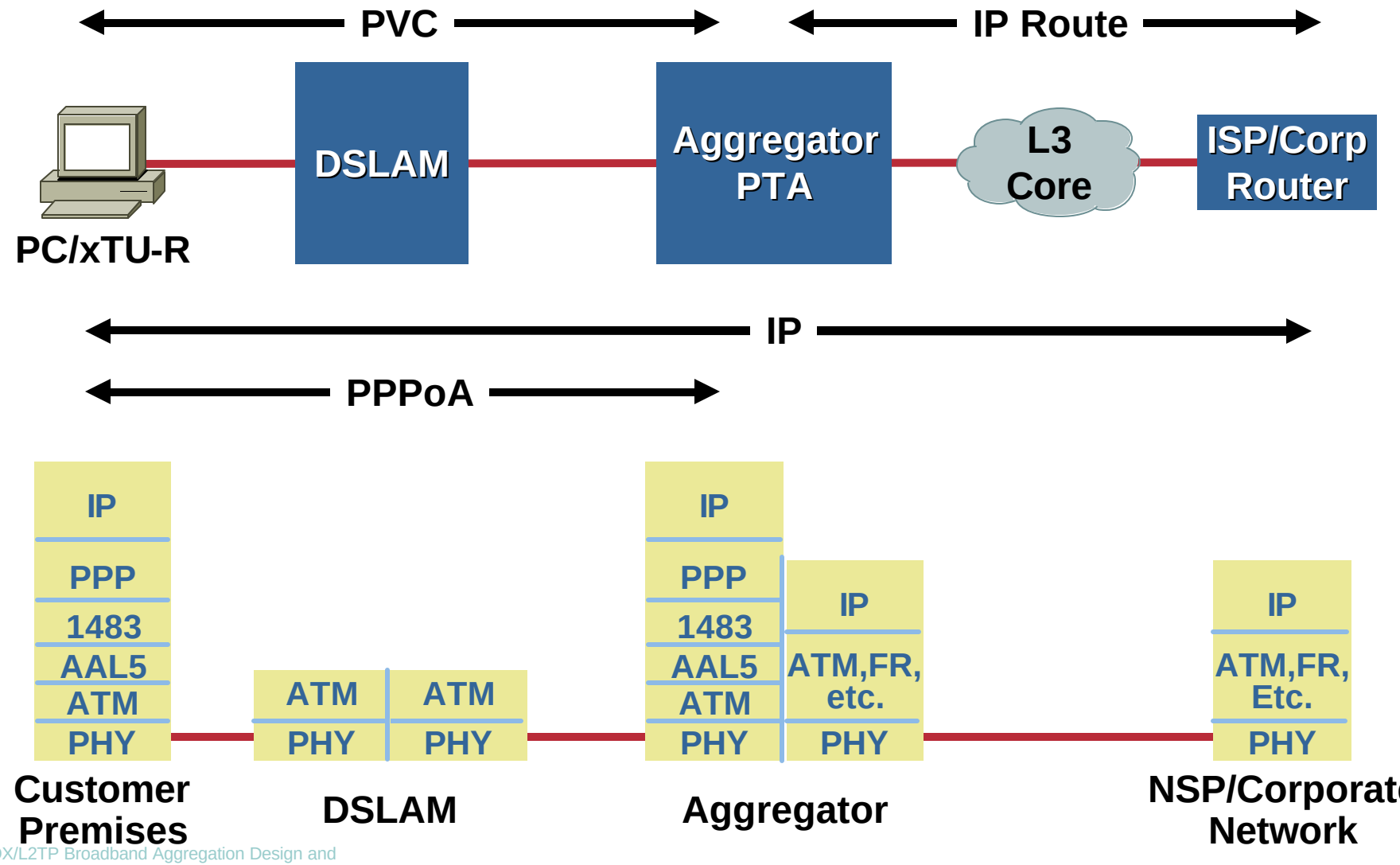
- **Access methods introduction**
  - **PPPoA**
  - **PPPoE**
    - **PPPoEoE/PPPoEo802.1q**
  - **L2TP**
  - **RBE**
- **Scaling on Cisco BB platforms**
  - **VC range**
  - **VC class**
  - **PVC auto provisioning**
  - **Auto Sense**
  - **BB Groups**
  - **Per-User Service Differentiation Using AAA**
- **BB Services Offer**
  - **Personal Portals**
  - **Building intelligent pipes**
  - **Dynamic Bandwidth selection**
  - **QoS**
  - **Per subscriber Security Services**

Typical PPPoA Architecture

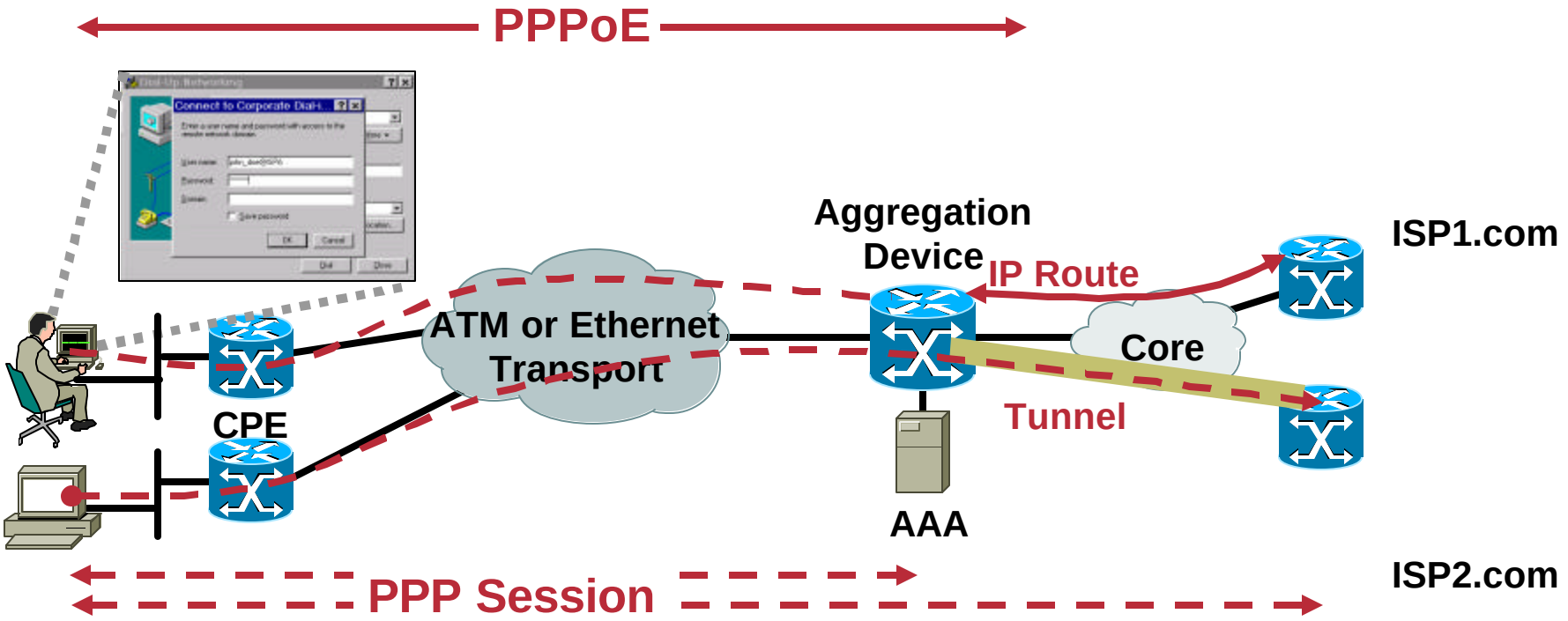


- PPP session initiated from CPE
- Authentication handled by aggregator or RADIUS server
- Aggregator routes or tunnels to services

PPPoA with PTA Protocol Stack

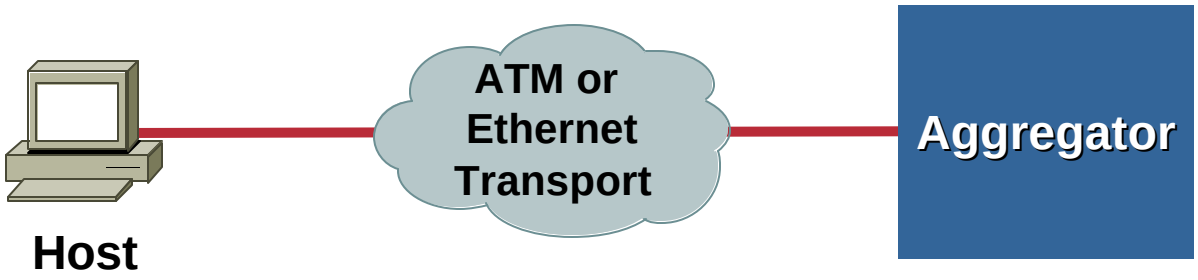


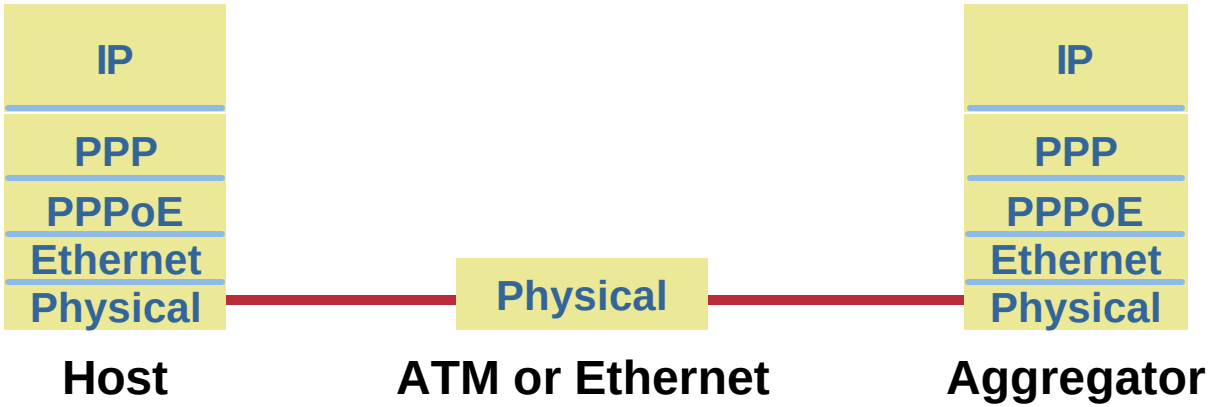
Typical PPPoE Architecture



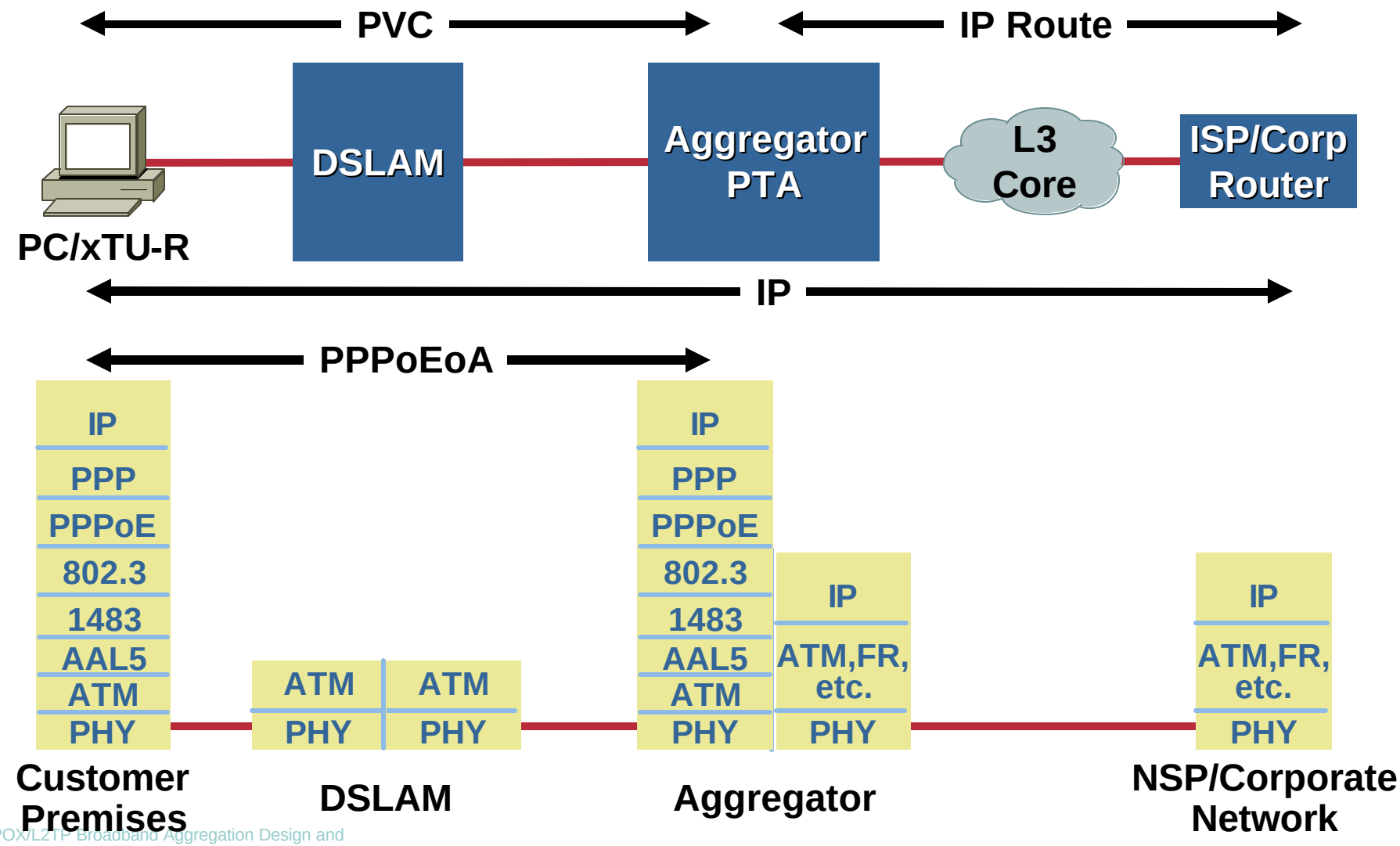
- PPPoE provides point-to-point connection over Ethernet
- Uses PPP dial in function on client
- Architectures include PPPoEoA, PPPoEoE, PPPoEo802.1q
- PPP session initiated from host
- Authentication handled by aggregator or RADIUS server
- Aggregator routes or tunnels to services

PPPoE Protocol Stack

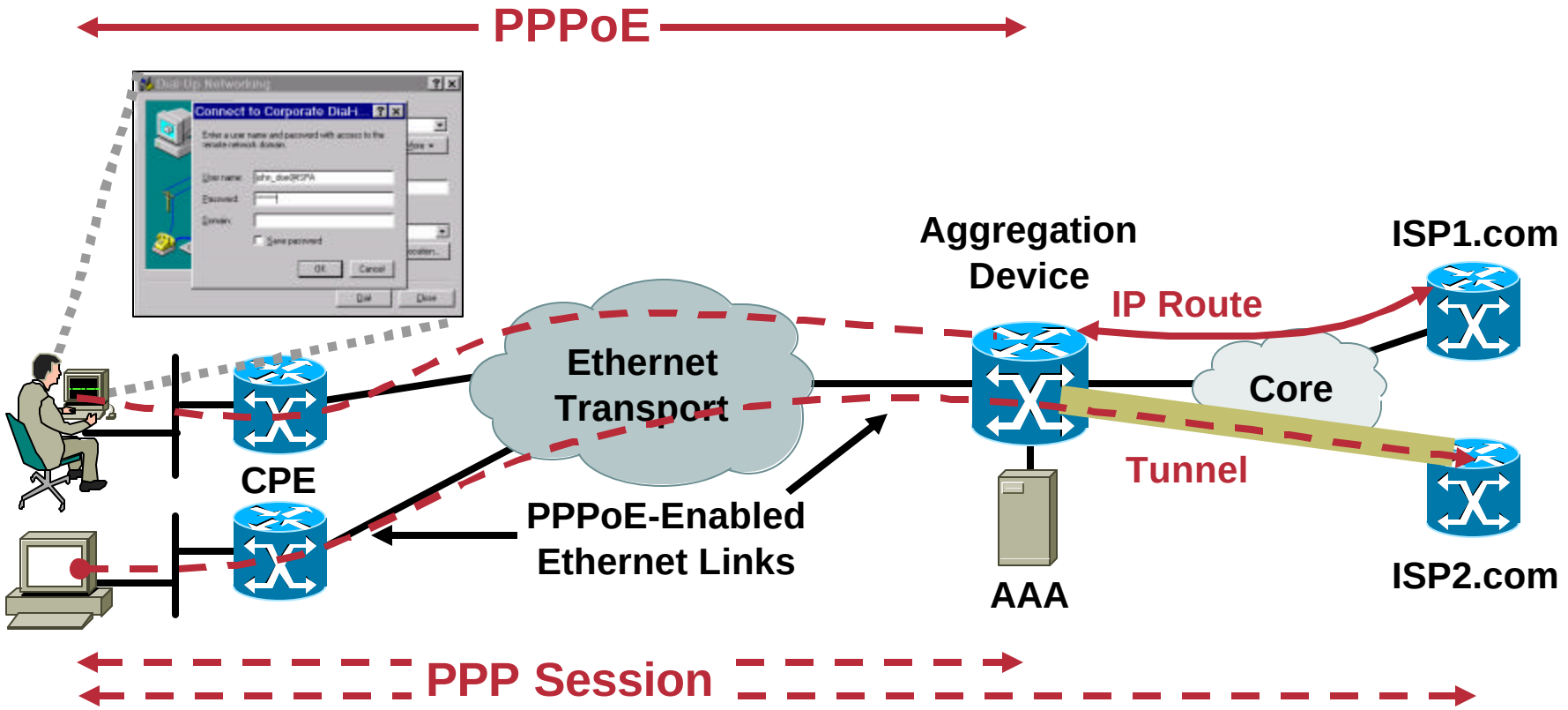




PPPoEoA with PTA Protocol Stack

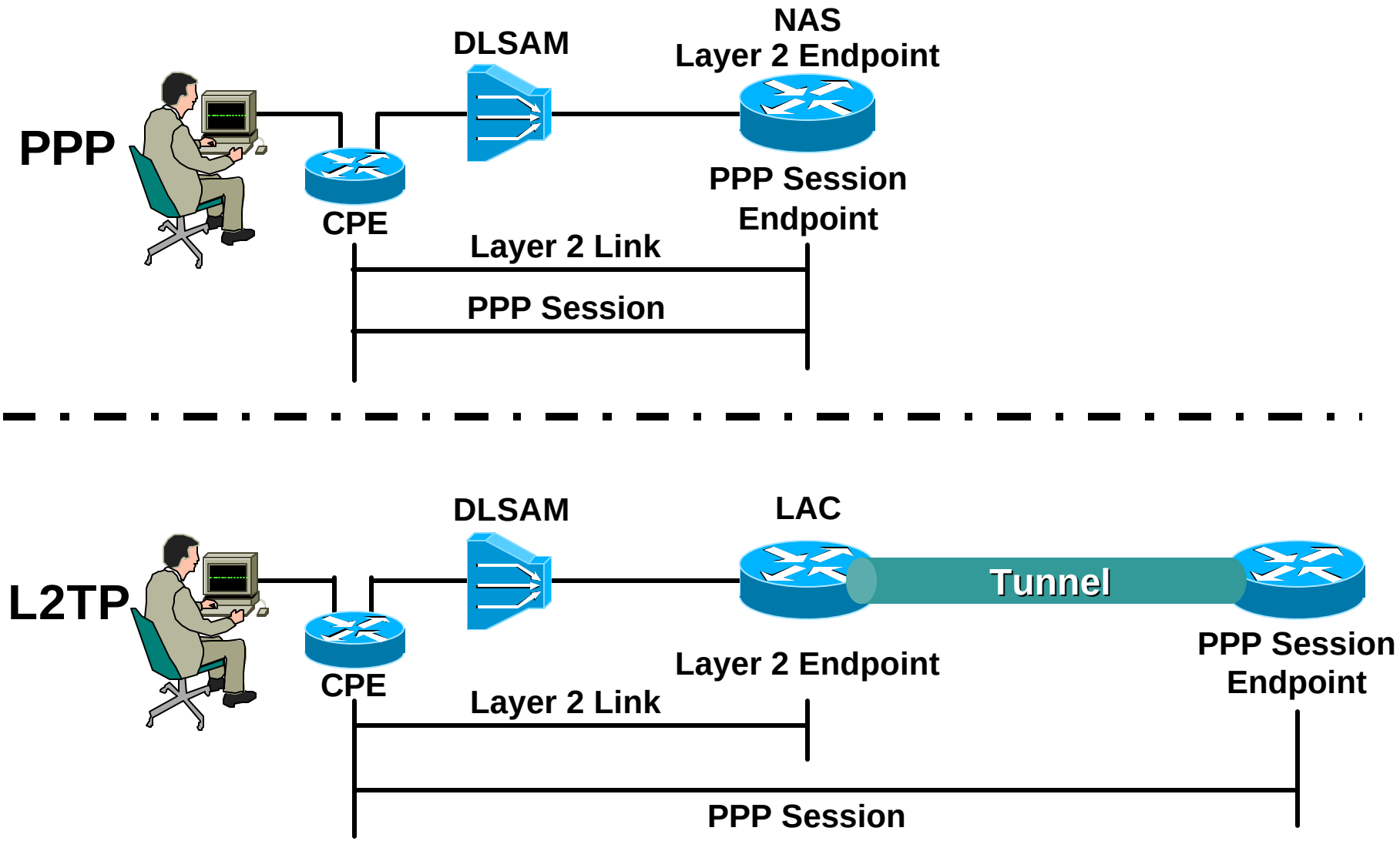


PPPoEoE and PPPoEo802.1q

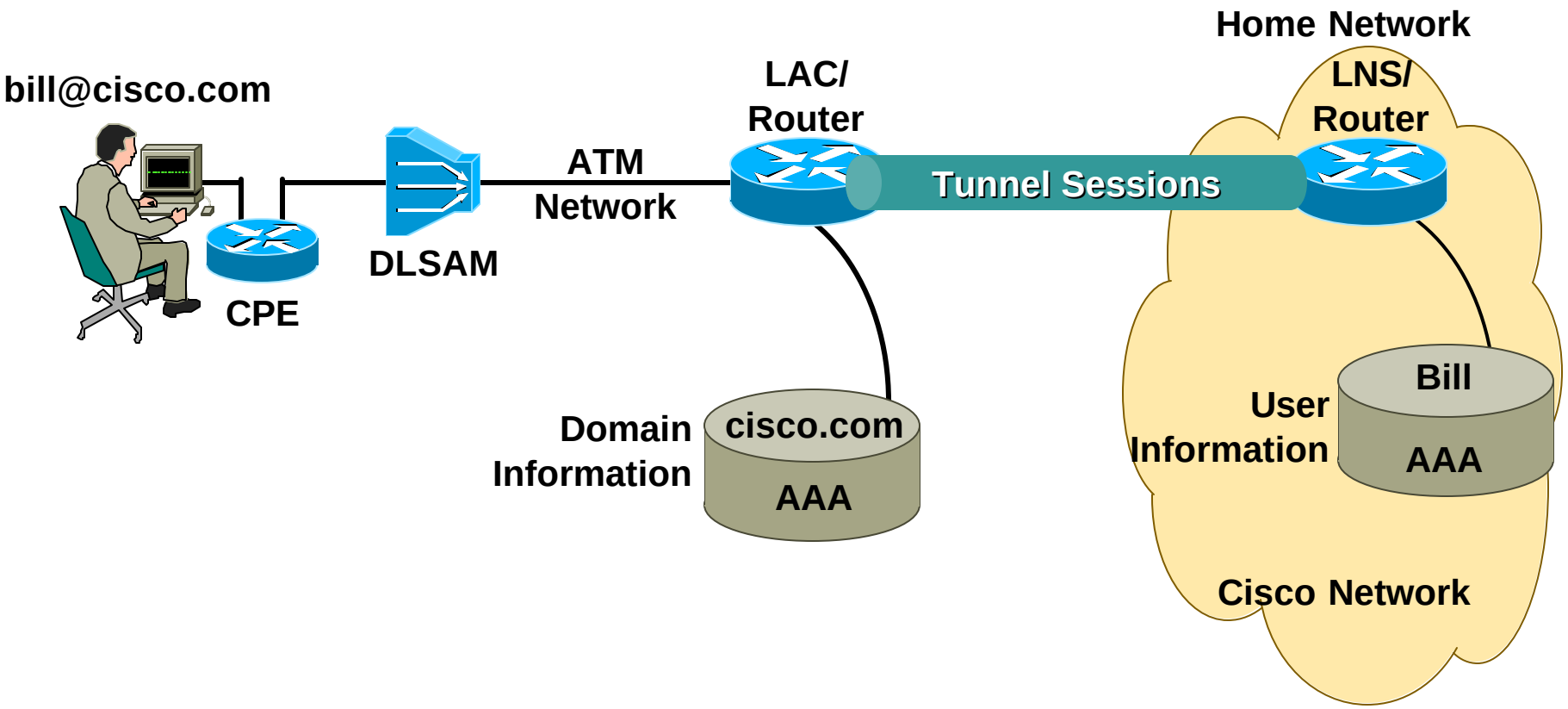


- Enhances PPPoE architectures by providing direct connections to Ethernet interfaces
- Common in metro Ethernet deployments
- ATM is no longer used in the access network

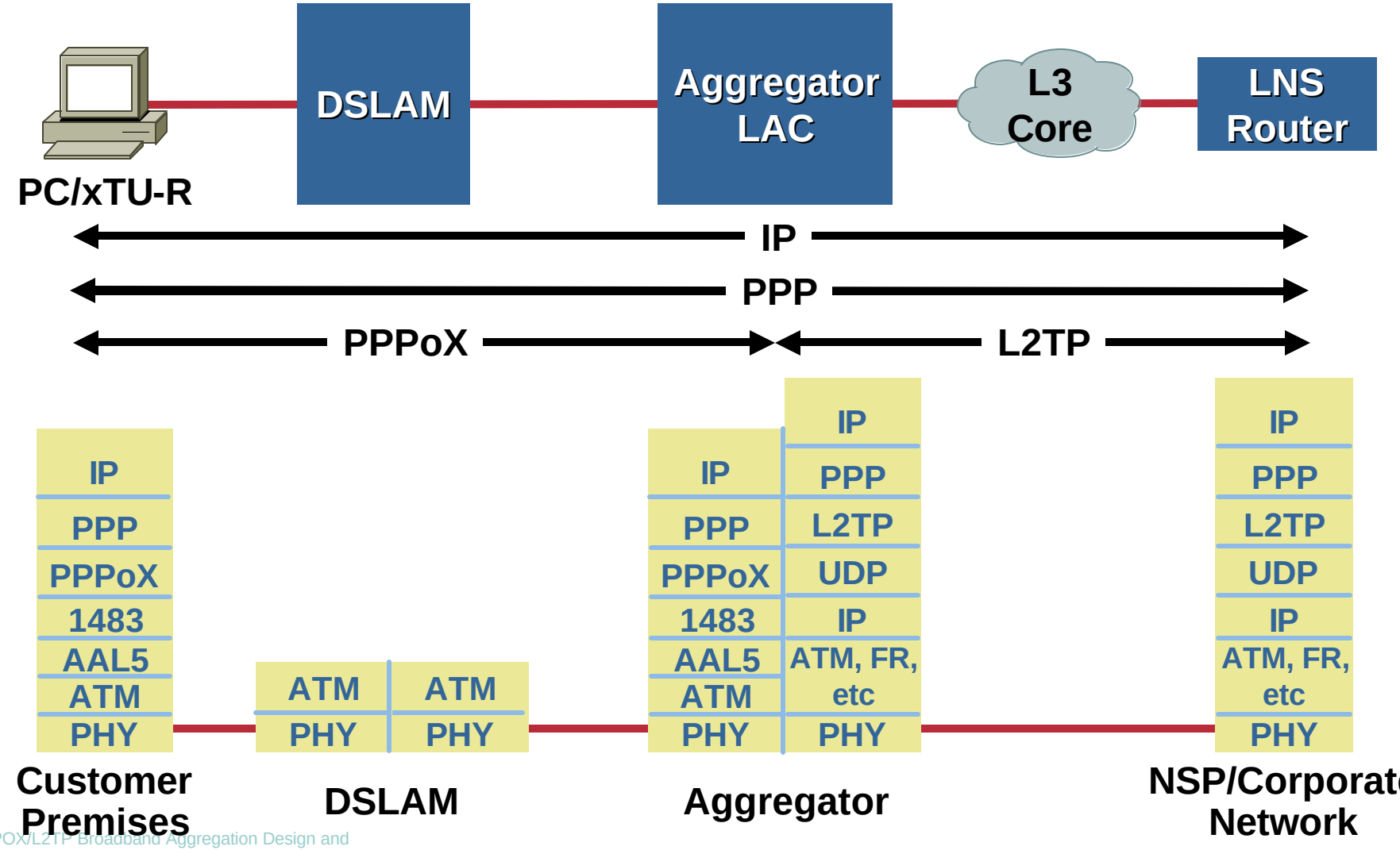
L2TP Overview



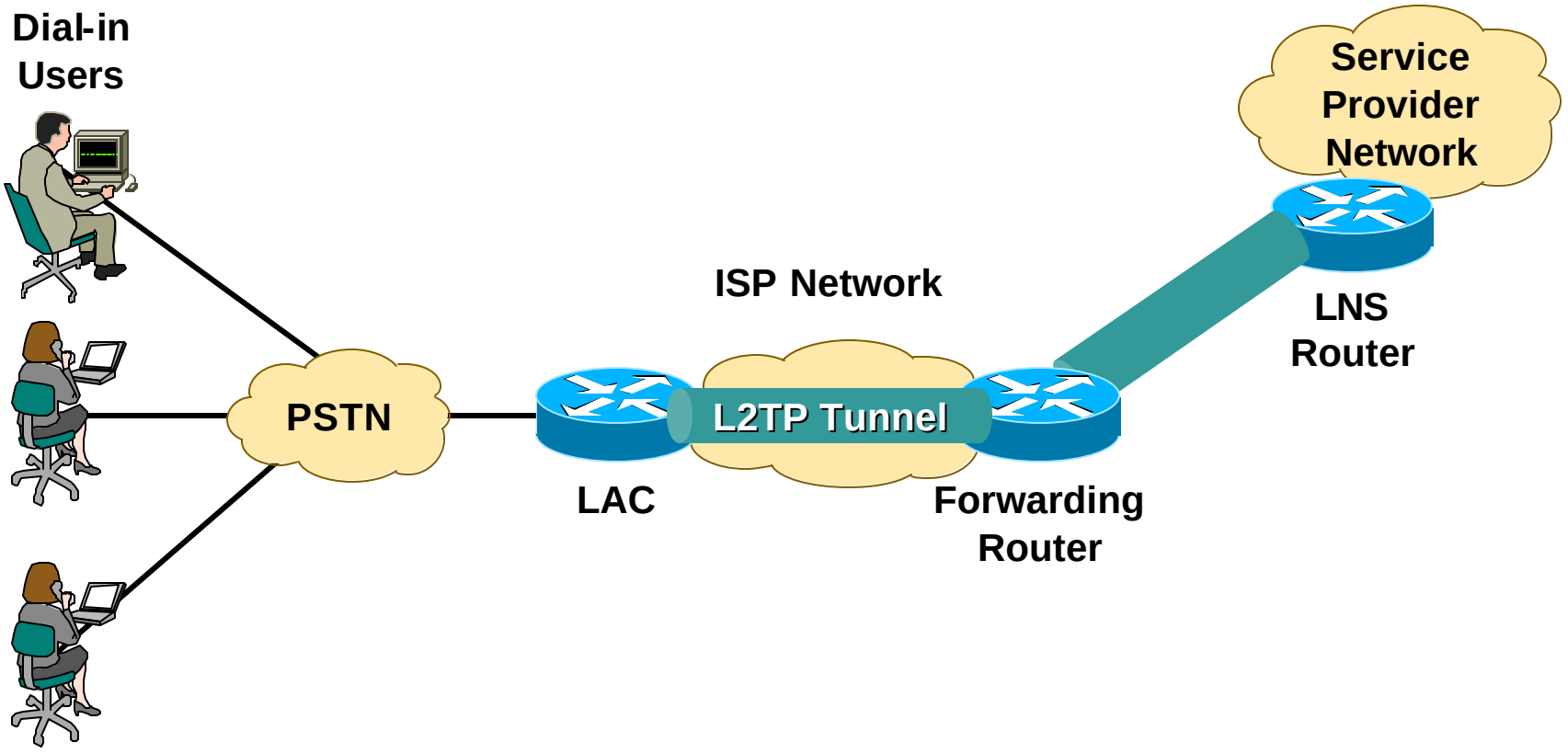
L2TP Components



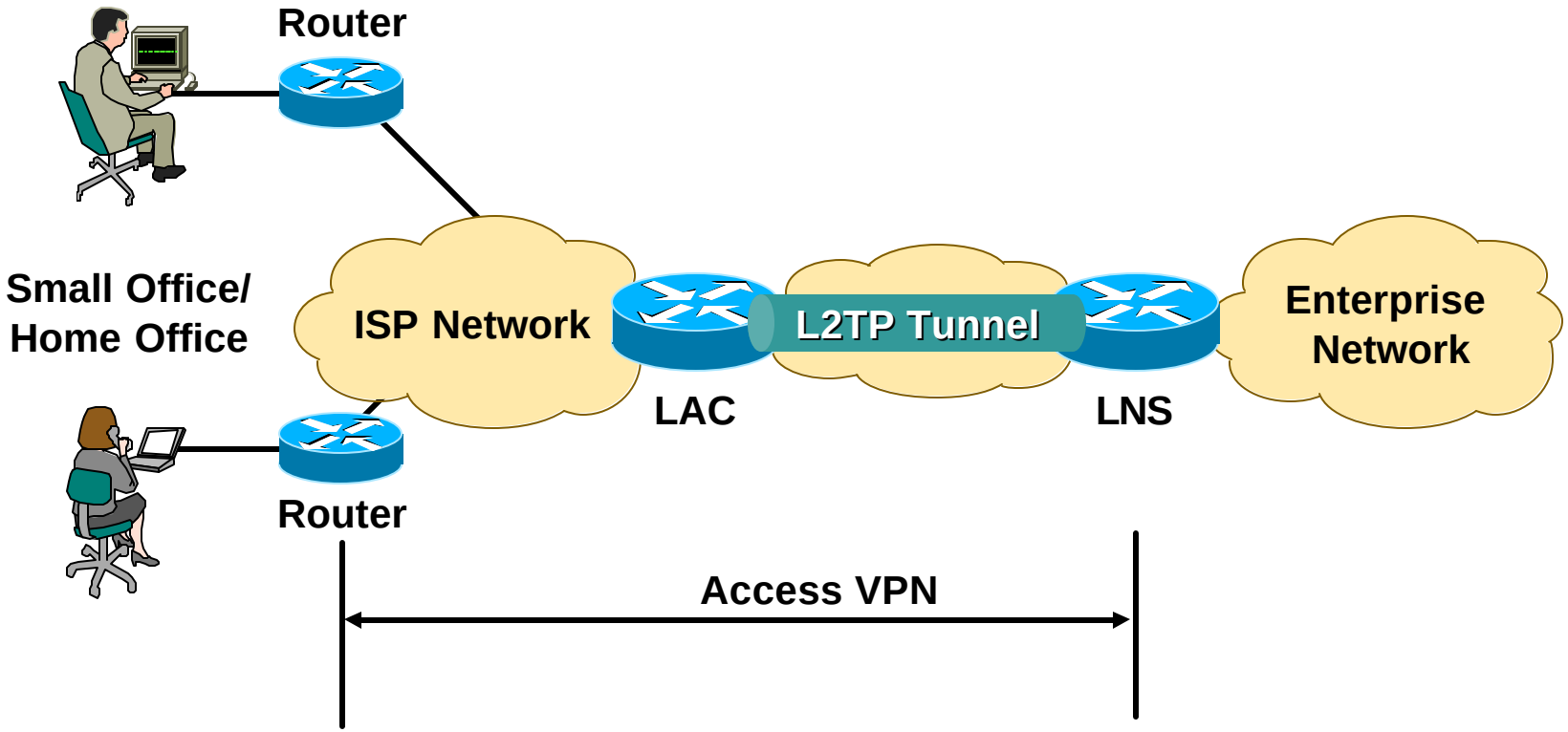
L2TP Protocol Stack



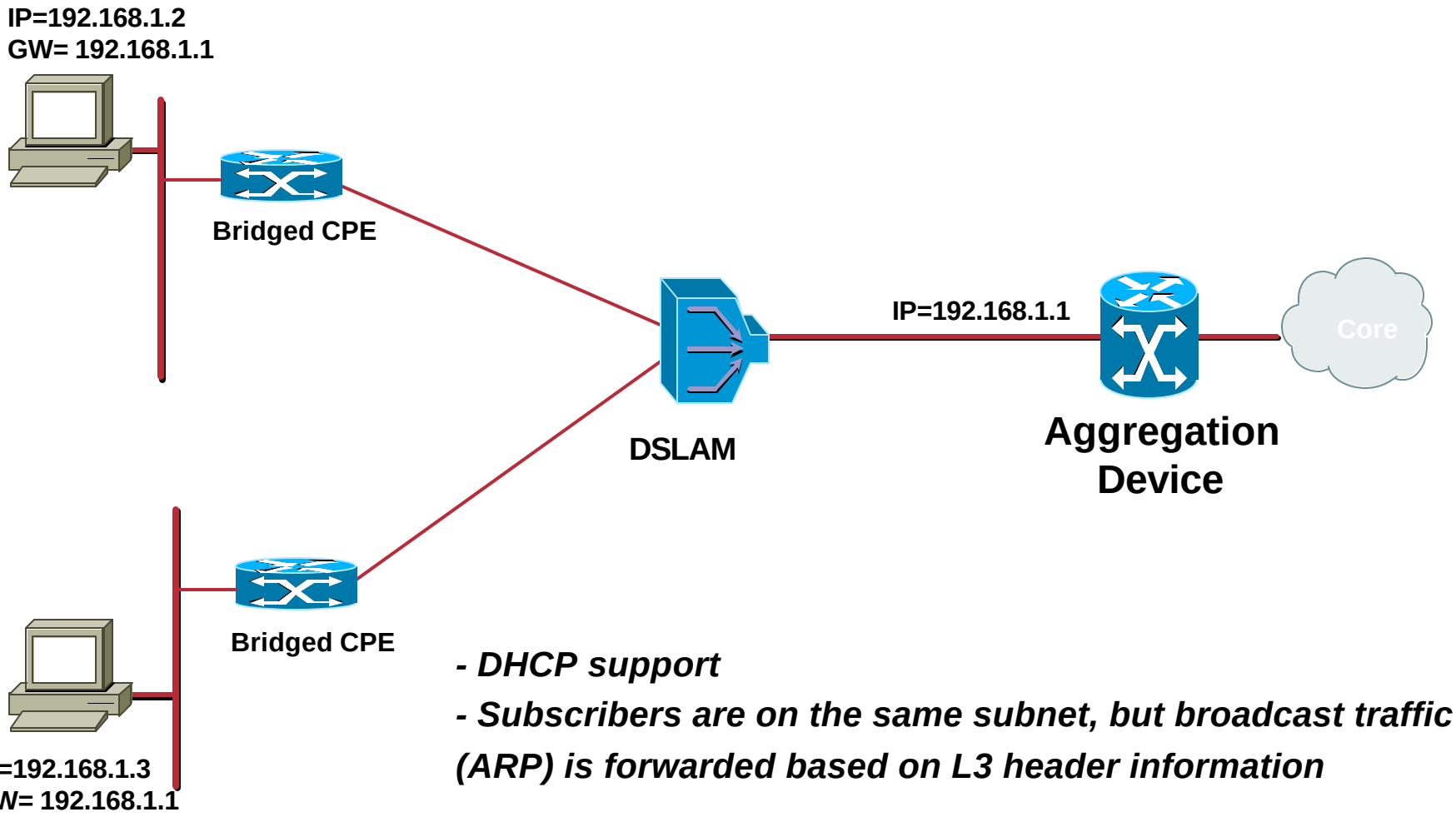
Wholesale Dial-in for Service Providers



Remote Access to Enterprise Network



RBE with unnumbered interfaces



- DHCP support

- Subscribers are on the same subnet, but broadcast traffic (ARP) is forwarded based on L3 header information

How does RBE work ?

- Subscriber traffic is carried in a BPDU
- Router looks at IP header and routes to destination
- ARP requests are only forwarded on correct VC

  router keeps a VC/MAC address table
- Multicast traffic is only forwarded on the interface where an IGMP join was received
- No spanning tree
- CPE is standard bridge

Agenda

- **Access methods introduction**
  - **PPPoA**
  - **PPPoE**
    - **PPPoEoE/PPPoEo802.1q**
  - **L2TP**
  - **RBE**
- **Scaling on Cisco BB platforms**
  - **VC range**
  - **VC class**
  - **PVC auto provisioning**
  - **Auto Sense**
  - **BB Groups**
  - **Per-User Service Differentiation Using AAA**
- **BB Services Offer**
  - **Personal Portals**
  - **Building intelligent pipes**
  - **Dynamic Bandwidth selection**
  - **QoS**
  - **Per subscriber Security Services**

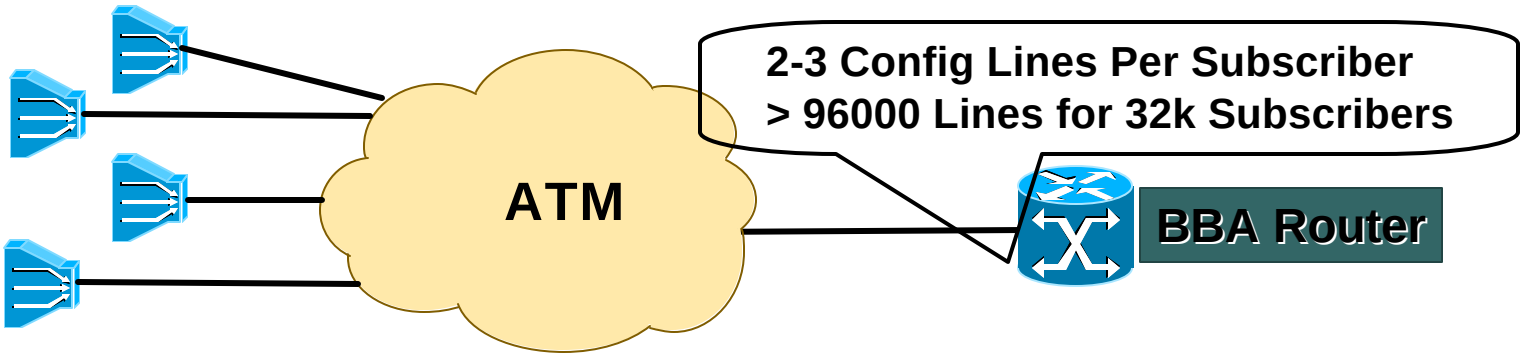
Scaling on Cisco BB platforms

Features that optimize router configuration and performance

- Methods to minimize ATM PVC provisioning
  - PVC range
  - VC class
  - ATM PVC autoprovisioning
- PPPoA Listen Mode
- Auto-sense PPPoX encapsulation
- PPPoE profiles

Subscriber VC Provisioning—The Traditional Way

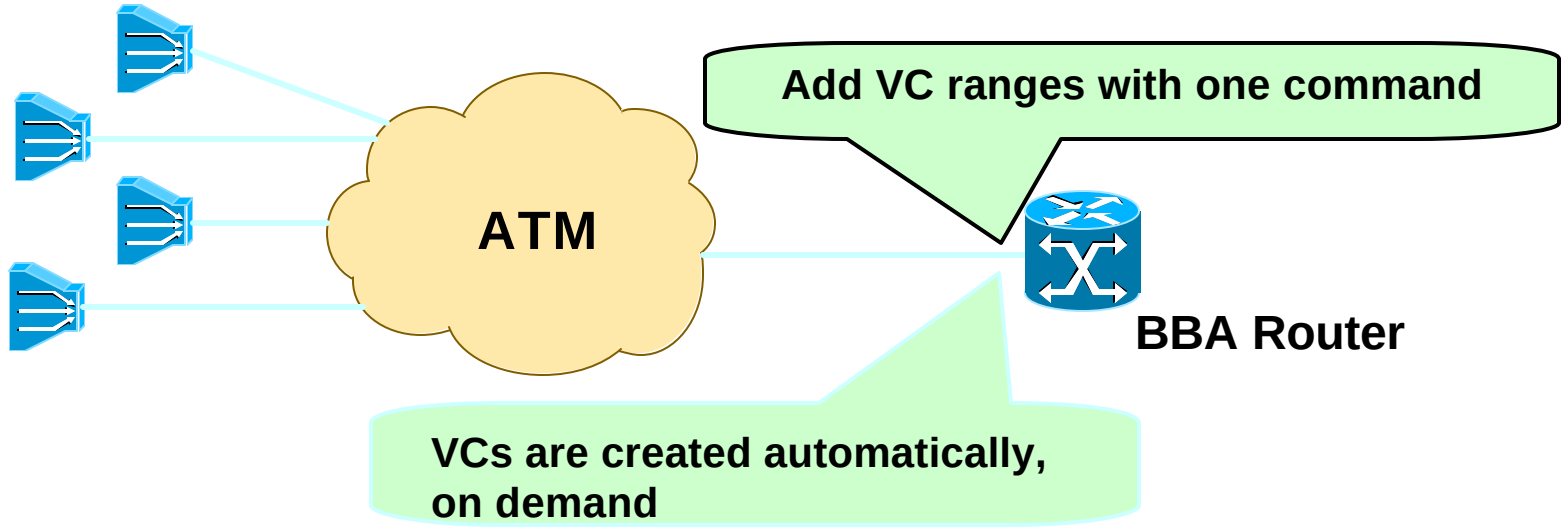
- **Subscriber VC provisioned at**
  - **DSLAM**
  - **BB aggregation router**
    - **Large # of VCs (as many as 8K, 16K, 32K subscribers)**
    - **2-3 lines per VC (24000, 48000, 96000 config lines!)**



- **Increased VC provisioning efforts at BBA router**
- **Difficulty in managing configuration, trouble shooting**
- **All configured VCs created at boot-up (whether used or not)**
  - **Longer boot time to create VCs**
  - **Wasted router resource (for unused VCs)**

Auto VC

New way for VC Provisioning



- **vc range command** – adds a range of VCs with one command
- **create on-demand** - VCs created automatically when needed

New Way - Advantages

- VC range: minimizes VC provisioning effort
  - Single command can create all VCs of an interface
  - Reduces router config size by orders of magnitude
  - Eg., for 16000 subs, 3 lines per VC, 5 sets of VC shaping rates:
    - Old way: 16000x3 = 48000 lines
    - New way: 5 different ranges = 5 lines only!
  - Smaller config simplifies trouble-shooting
- Create on-demand - VCs are created on demand
  - Better resource utilization (e.g., memory)
  - Router boots faster, since VCs not created at boot-up

VC Class

Without VC Class

```
ATM int/subinterface
   PVC
      encapsulation
      QoS parameters
   PVC
      encapsulation
      QoS parameters
```

Using VC Class

```
Vc-class atm bronze
   encapsulation
   Qos parameters

ATM int/subinterface
   PVC
      class bronze
   PVC
      class bronze
```

- Set of preconfigured VC parameters
- Class associated with VC or ATM interface
- Specify QoS, encapsulation, and bandwidth parameters

Listen Mode for PPPoA Sessions

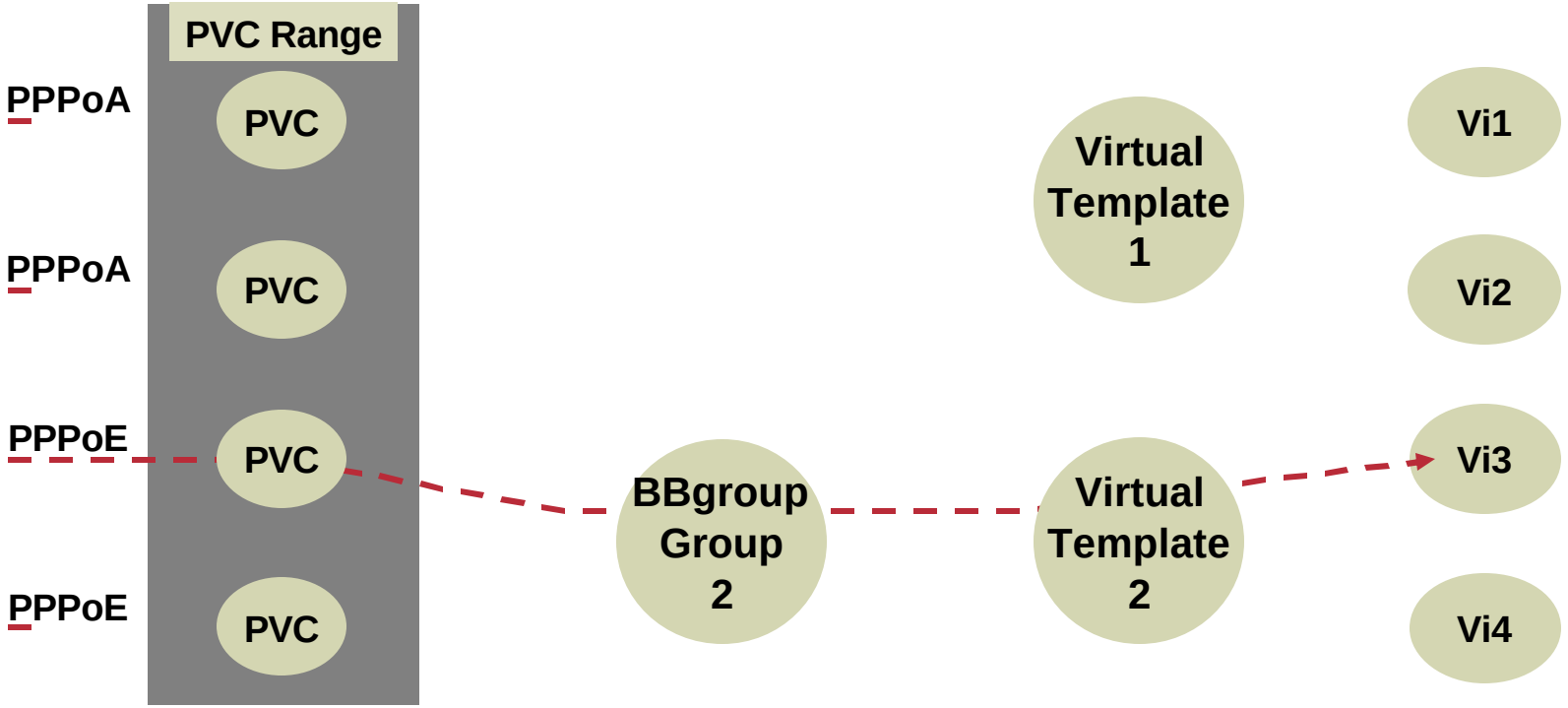
- PPPoA, PPPoEoA, or LAC , sessions may be placed in listen mode
- Reduces processing of all inactive sessions

Configuration Example

```
!
interface atm8/0/0.132 multipoint
 atm pppatm passive
 range pvc 1/32 2/4095
  encapsulation aal5mux ppp virtual-template1
!
```

Auto-sense PPPoX Encapsulation

Cisco.com



Distinguishes between PPPoA and PPPoE sessions

Works for SNAP and MUX encapsulation

Functions on PVC, PVC range or VC class

Saves configuration time and overhead on NAS

Cisco Zero-Touch Provisioning

What is it?

New Cisco capability that allows Virtual Circuits to be automatically setup (and taken down) with NO pre-provisioning

Problems

With no Auto-VC and PPP autosense:

- Memory is allocated when VC is configured – active or not
- No VC Over-provisioning
- Lack of flexibility when assigning VPI/VCI pair
- Increases router boot-up time

The Old Way (which wasn't too bad)

```
vc-class atm pppoa
  encapsulation aal5mux Virtual-Template1
!
interface ATM1/0
!
interface ATM1/0.1 multipoint
  range pvc 4/32 4/8031
  class-range pppoa
!
interface ATM1/1
!
interface ATM1/1.1 multipoint
  range pvc 5/32 5/8031
  class-range pppoa
```

Cisco Zero Touch Provisioning

The New Way

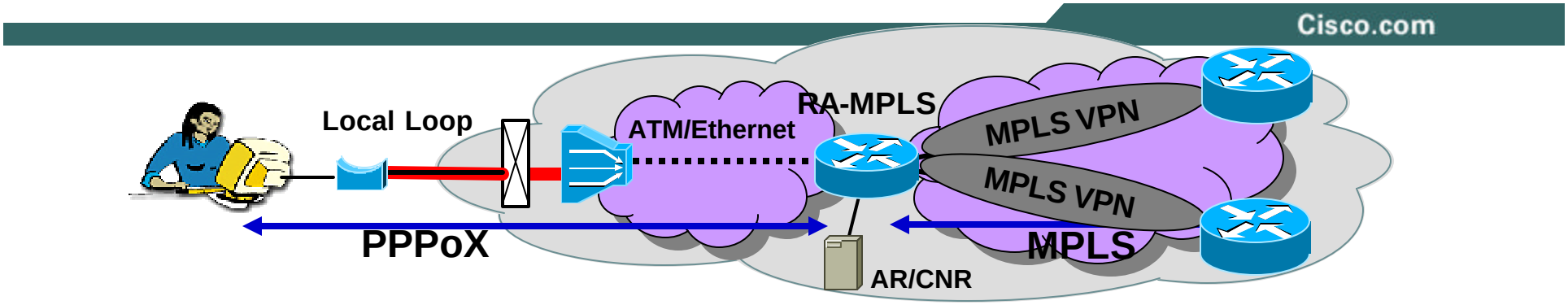
```
vc-class atm zerotouch
  encapsulation aal5autoppp Virtual-Template1
  create on-demand
!
interface ATM1/1
   pvc 1/32
  class-int zerotouch
```

Benefits

Using the new Cisco ability to create ATM VCs automatically and the new Cisco ability to autosense ATM encapsulation:

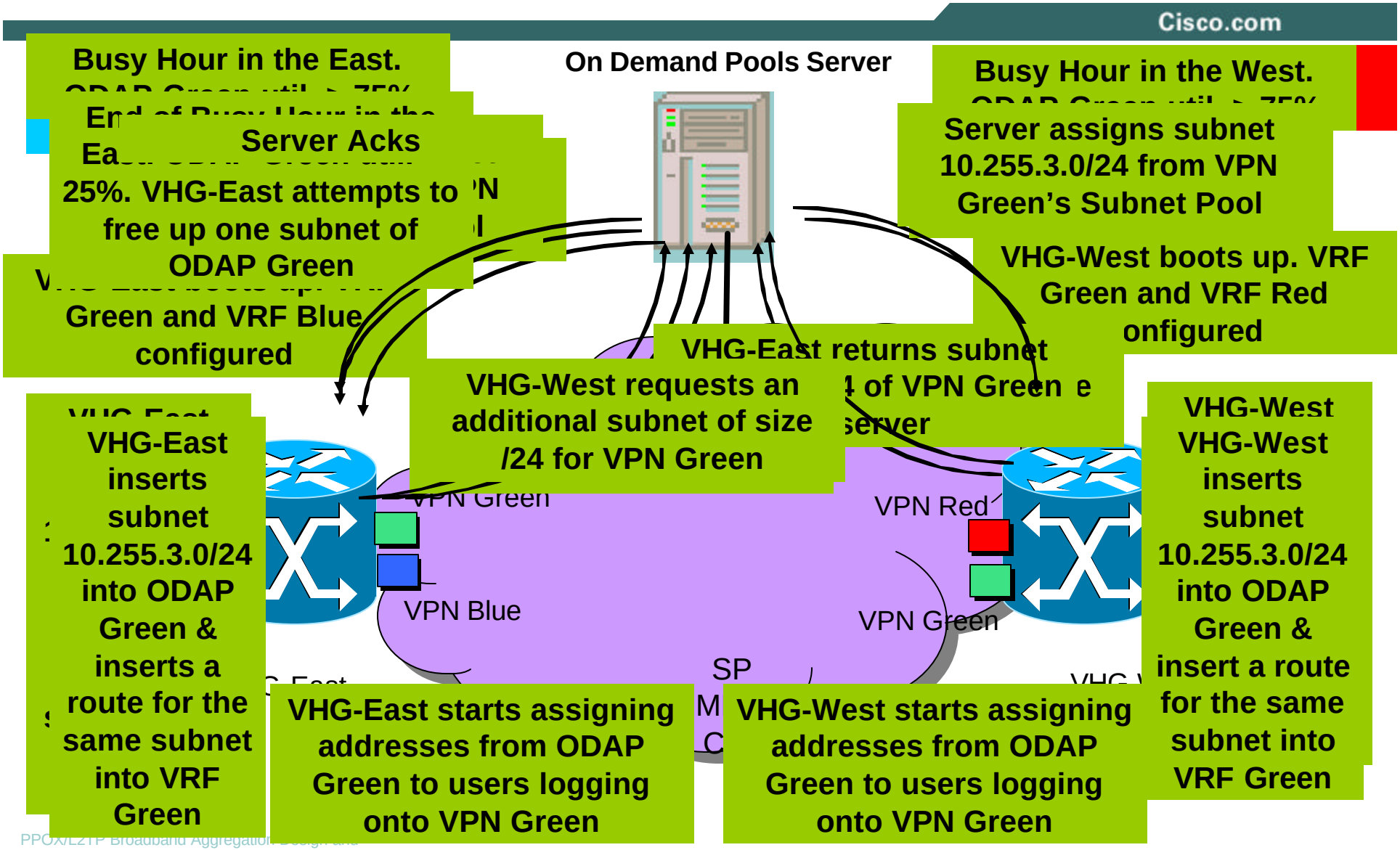
- **Memory is only allocated when VC is active**
- **Allows for TRUE ATM VC Over-provisioning**
- **Any VPI/VCI pair can be used on the interface**
- **Supports both PPPoA and PPPoE subscribers**

On-demand Address Pools

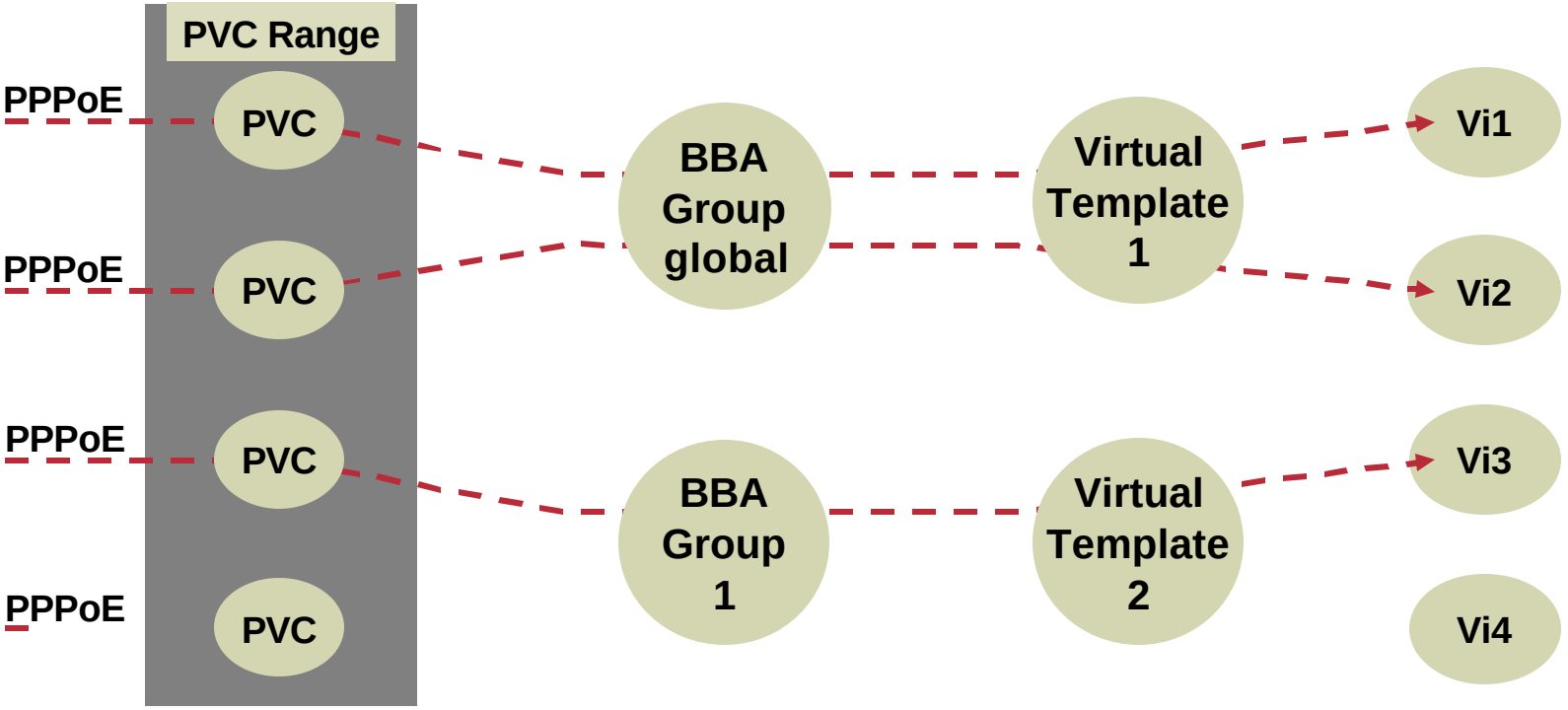


- IP address pools for each VRF
- Uses Radius (AR) or DHCP (CNR) to assign Clients IP address based on a VRF
- Overlapping IP address Pools is possible
- Local defined address Pool for each VRF
- Radius (AR) or DHCP (CNR) manages IP assignment out of the local address Pools
- Available on IOS

On Demand Address Pools



PPPoE Profiles



VPDN group permits only one group for PPPoE

BBA group allows multiple groups for PPPoE

Applies to interfaces, PVC, PVC range, PVC-in-range, VC class, PPP auto-sense

PPPoE Features

Multiple PPPoE Group support

Before BBA-GROUP

```
vpdn-group 1
accept-dialin
protocol pppoe
virtual-template 1
interface atm7/0/0.1 multipoint
range pvc 10/32 10/2031
protocol pppoe
Range pvc 11/32 11/2031
protocol pppoe
```

Now

```
bba-group pppoe customerA
virtual-template 1
!
bba-group pppoe customerB
virtual-template 2
!
interface atm7/0/0.1 multipoint
range pvc 10/32 10/2031
protocol pppoe group CustomerA
Range pvc 11/32 11/2031
protocol pppoe group CustomerB
```

Per-User Service Differentiation Using AAA

1. Some per-user parameters are downloaded using specific VSAs
2. A few downloaded using lcp:interface config:
   - QoS parameters: service policy, CAR
   - Bandwidth: DBS
   - Security: ACLs, uRPF
   - Downloading routes
   - Downloading VRF names
3. Scalability impact of lcp:interface-config
   - Commands have to be parsed when calls are brought up
   - New VSAs to improve scalability of service policy, VRF name

Per-User Service Differentiation Using AAA

- VSAs 37/38 for service policy download
- Allows downloading QoS policy name from RADIUS server
- Available 12.2(15)B
- Policies are defined locally on the router
- Scales much better than lcp:interface-config

Per-User Service Differentiation Using AAA

VSA Type 37 – Upstream Traffic to Input policy name

peruser_qos_1 Password = "lab"

Service-Type = Framed,

Framed-Protocol = PPP,

Cisco:Cisco-Policy-Up ="policy_class_1_2"

VSA Type 38 – Downstream traffic to Output policy name

peruser_qos_2 Password = "lab"

Service-Type = Framed,

Framed-Protocol = PPP,

Cisco:Cisco-Policy-Down ="policy_class_1_2"

Per-User Service Differentiation Using AAA

Scaling for MPLS VPN

New Cisco-AV pair to avoid lcp:interface-config scaling issue

Old Profile:

- **Cisco:Cisco-Avpair = "lcp:interface-config=ip vrf forwarding coke"**
- **Cisco:Cisco-Avpair = "lcp:interface-config=ip unnumbered Loopback 0"**

New Profile:

- **Cisco:Cisco-Avpair = "ip:vrf-id=coke"**
- **Cisco:Cisco-Avpair = "ip:ip-unnumbered=Loopback 0"**

Agenda

- **Access methods introduction**
  - **PPPoA**
  - **PPPoE**
    - **PPPoEoE/PPPoEo802.1q**
  - **L2TP**
  - **RBE**
- **Scaling on Cisco BB platforms**
  - **VC range**
  - **VC class**
  - **PVC auto provisioning**
  - **Auto Sense**
  - **BB Groups**
  - **Per-User Service Differentiation Using AAA**
- **BB Services Offer**
  - **Personal Portals**
  - **Building intelligent pipes**
  - **Dynamic Bandwidth selection**
  - **QoS**
  - **Per subscriber Security Services**

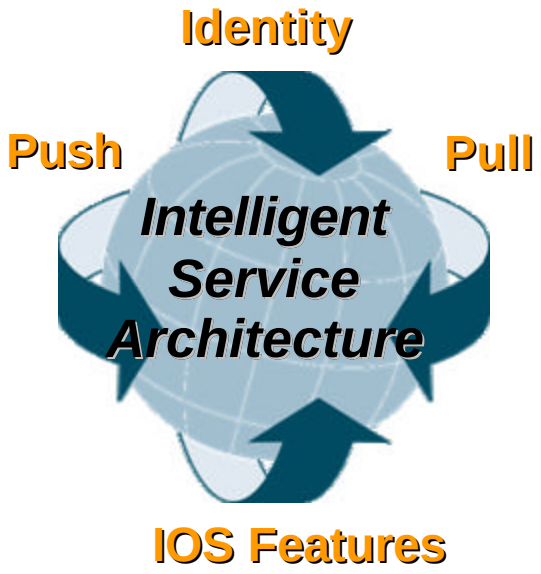
Intelligent Service Architecture

Generic Session
With multi-dimensional identifier per session

Policy Plane
- Policy retrieval and distributi
- Identity Management
- Authentication/Autho
- Distributed compo

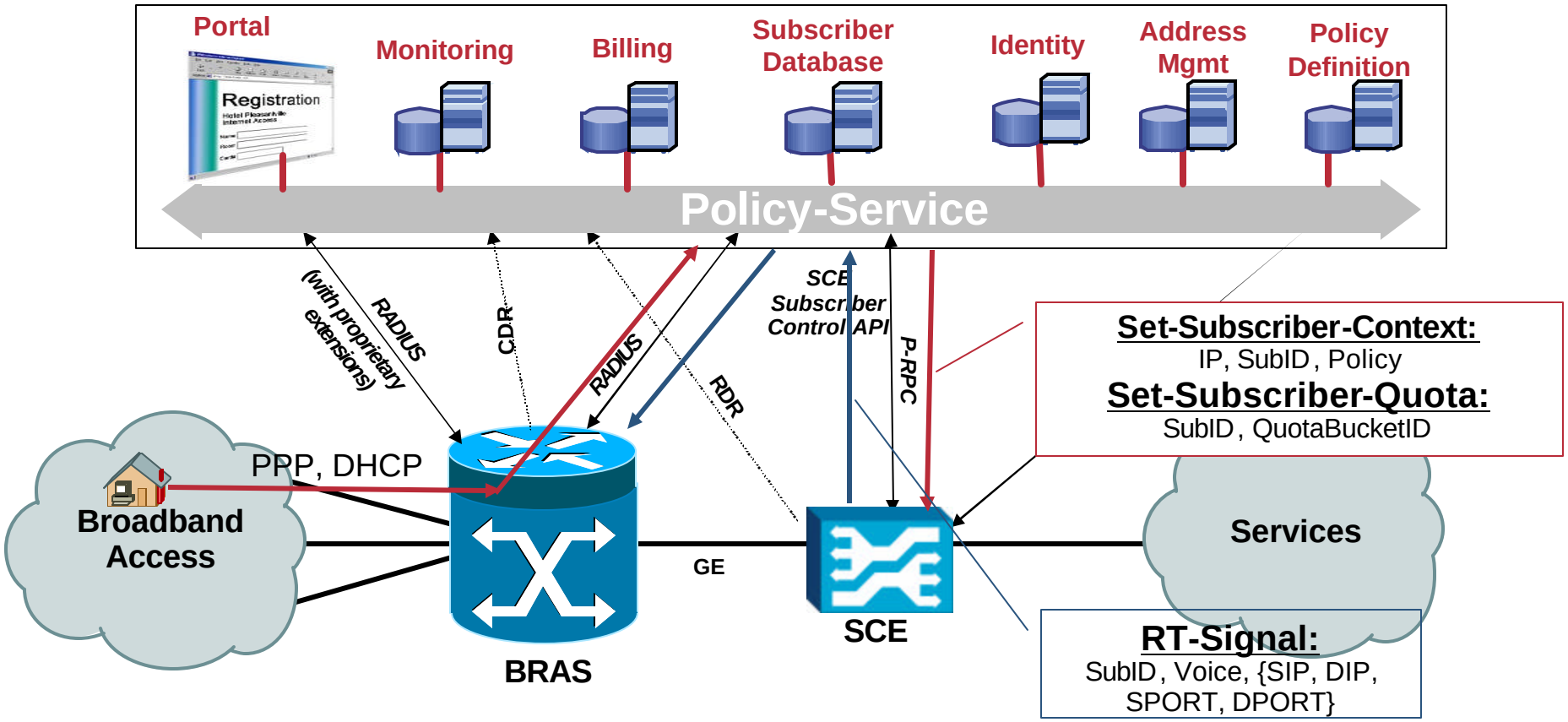
Control Plane
- Policy enforcement
- Data plane provisioning
- Event handling
- Platform independent

Data Plane
- Platform dependent
- Software switching (IOS)
- Switching Abstraction Layer (SAL)
- Hardware switching (C10k, 7600, 12000)



Data flows

The Abstracted Network - Low OPEX



-Setup Subscriber-Context on SCE on session establishment

-RT Signaling of L4 data to setup QoS on aggregator

Adding Subscriber Intelligence to IP Networks to increase per subscriber revenue

Revenue Generating Services

- Walled Garden Portal
- Subscriber Self-care portal & accounting
- PrePaid Services (Volume, time …)
- Turbo Button

- Protocol Restriction (no IPSEC)
- TCP Session Limits
- Per User Firewall

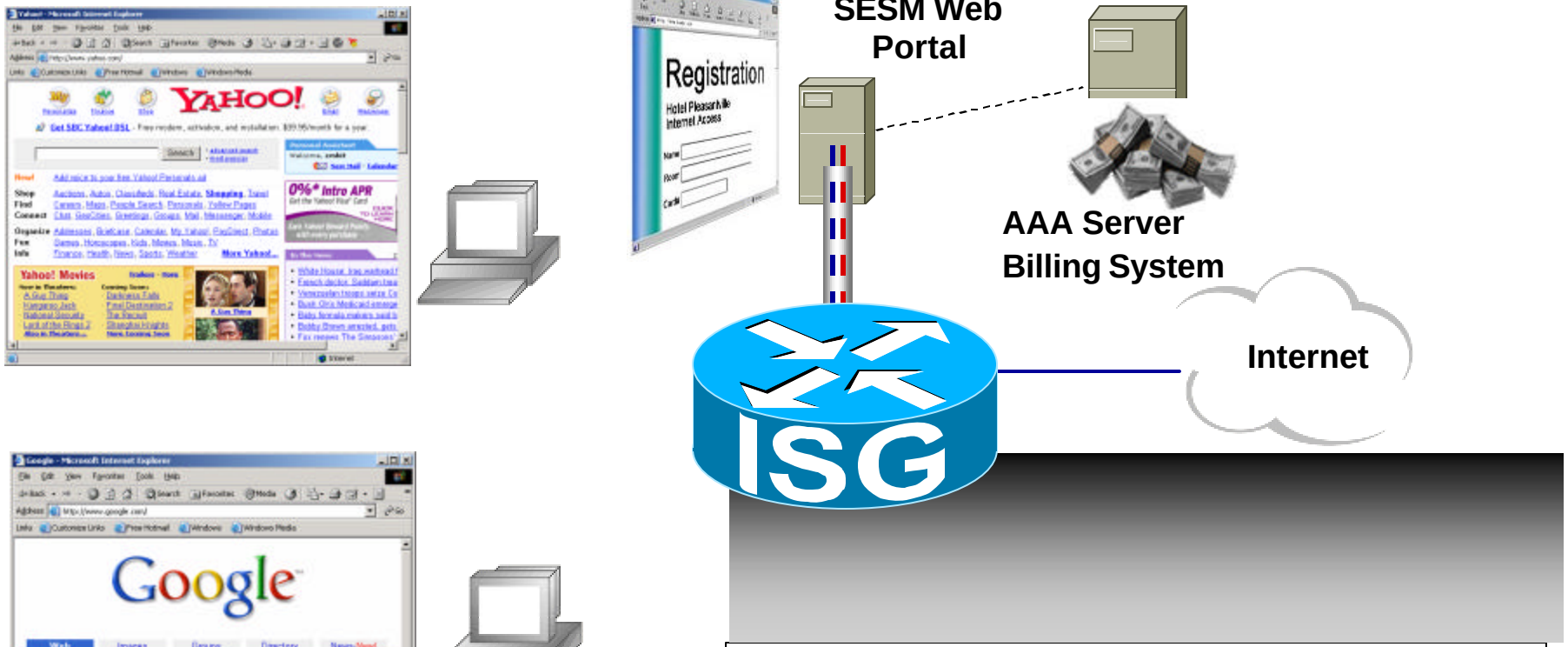
- Peer 2 Peer Traffic Marking
- Virus Filtering
- Traffic Pattern analysis

- User based billing
- Export data format for Billing Services
- Integrated to 3rd party billing

- SLA Monitor and reporting

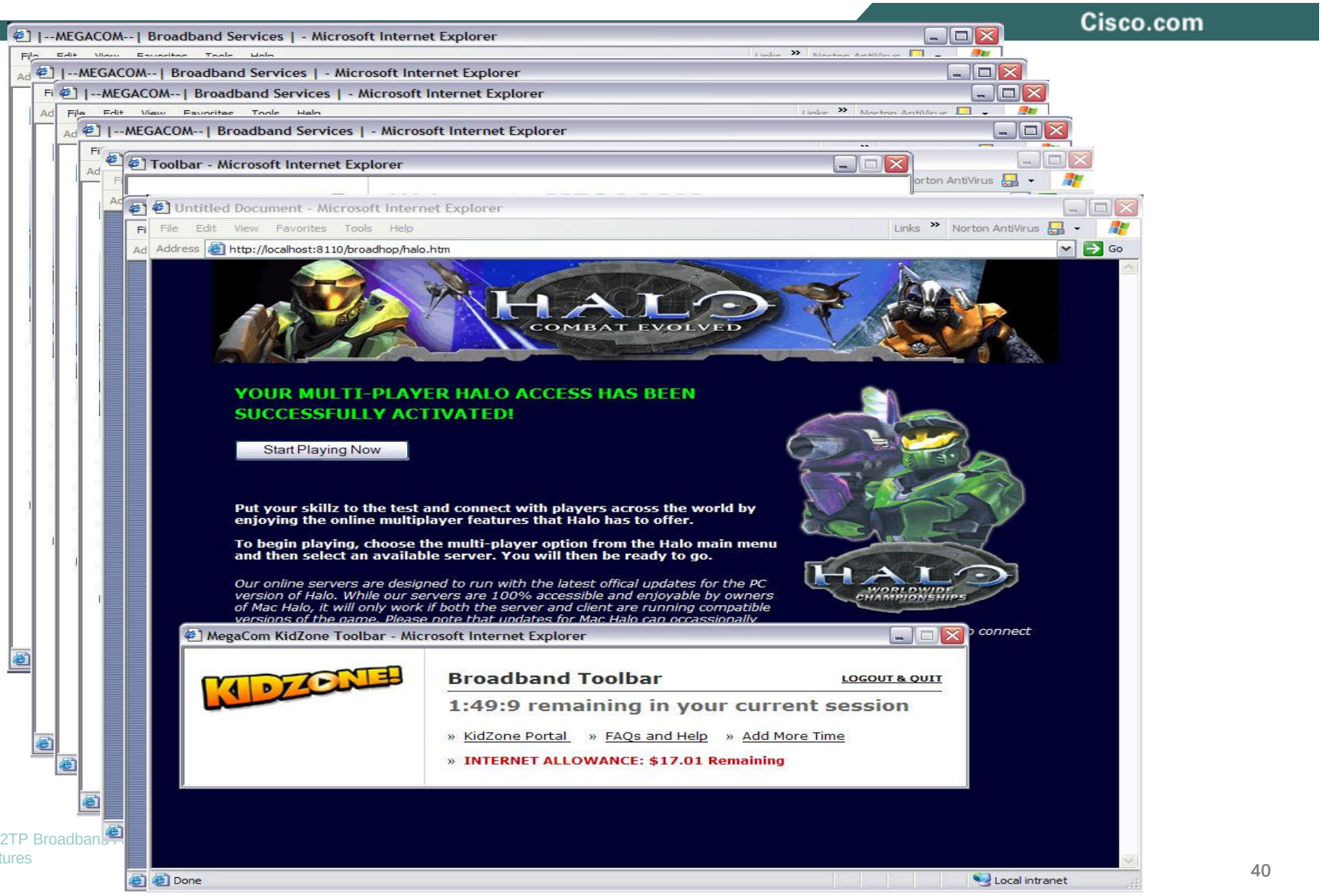
Personal Portals

Intercept Customers and force them to logon



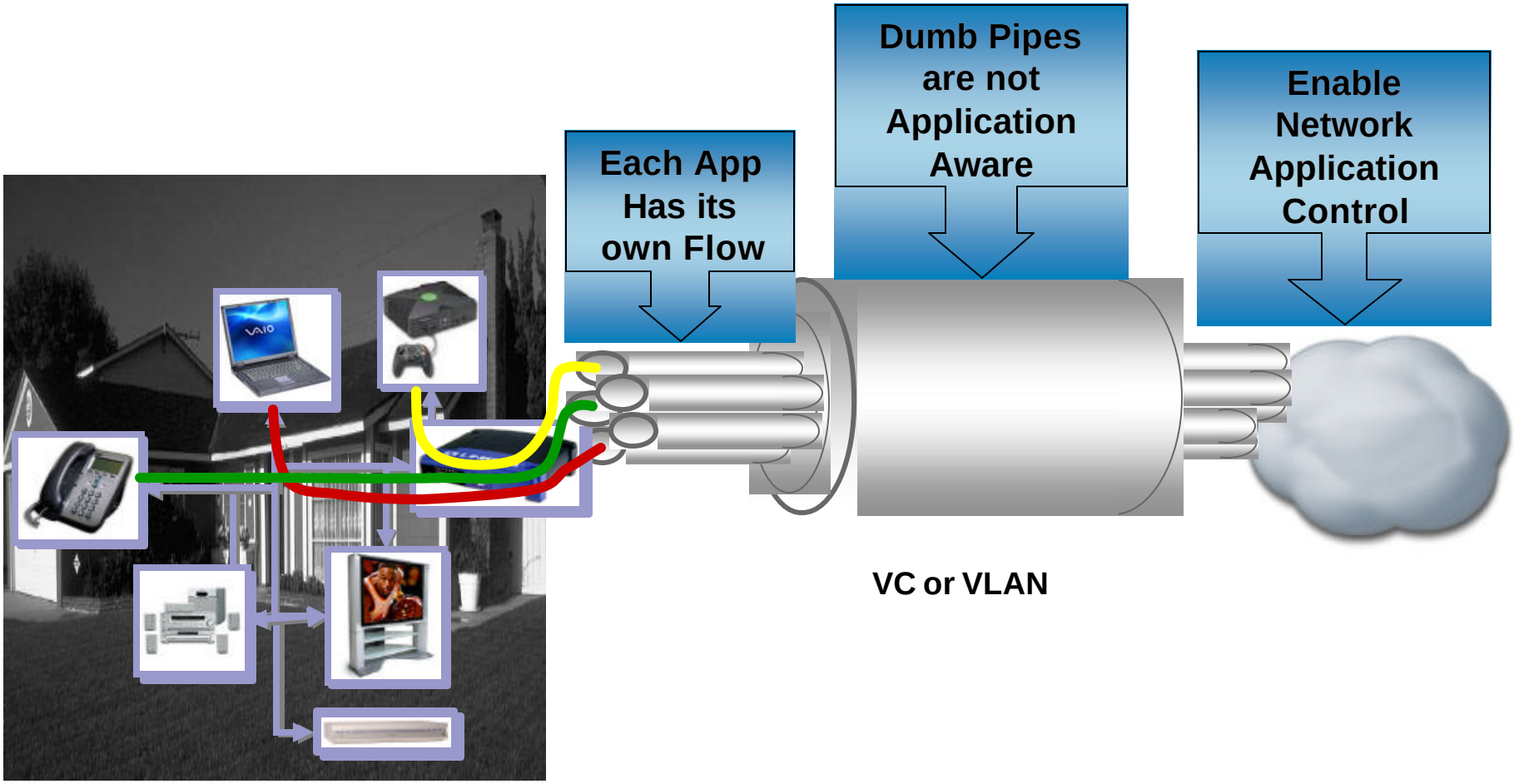
- Capture web sessions on start up or at configurable intervals
- Target advertising to identified subscribers
- Match content to identified subscribers

Subscriber Self Care
Default pages on Cisco Portal



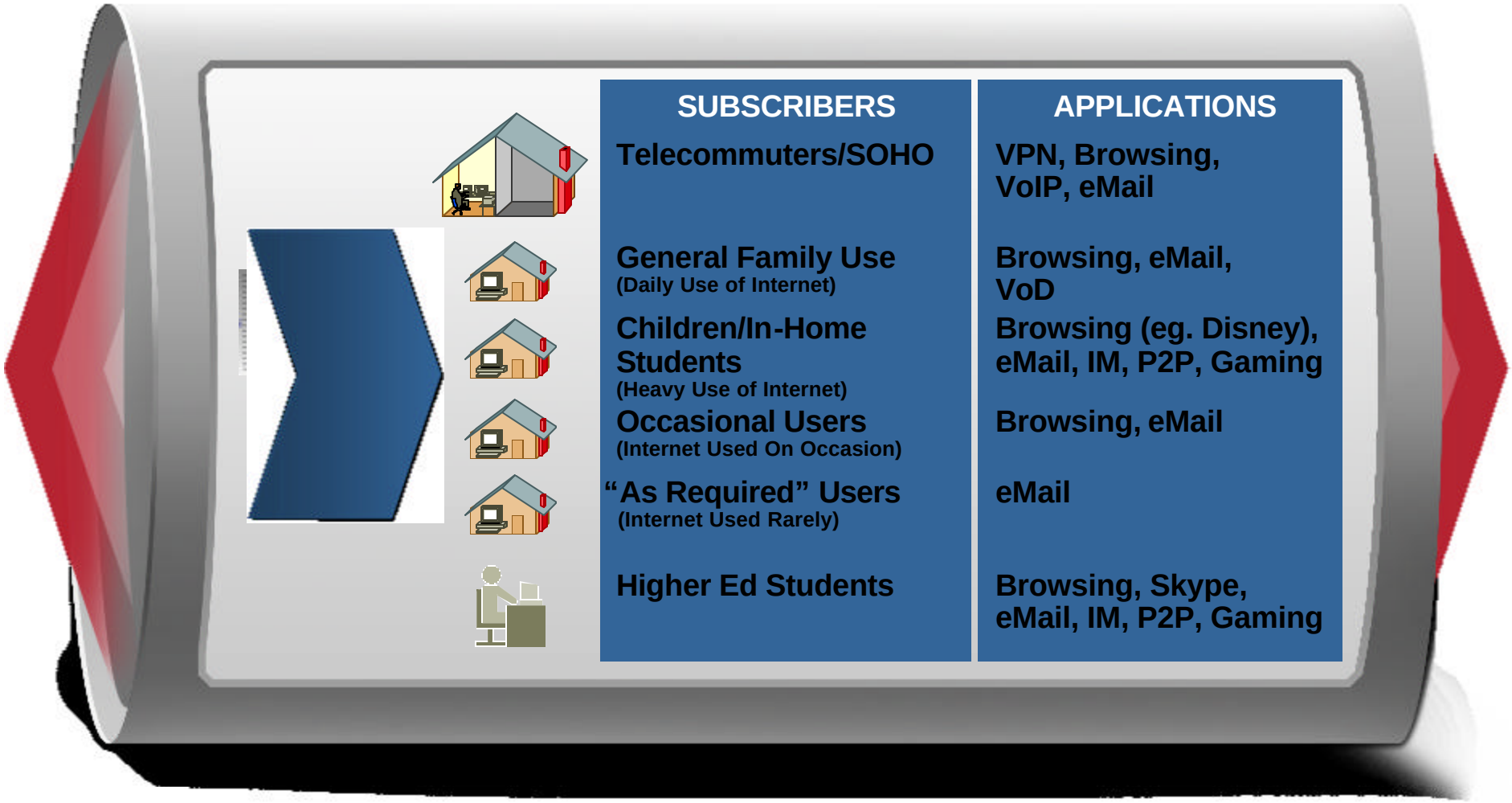
Building Intelligent Pipes

Network Based Application Control



Step 1: Usage Analysis

NETWORK PROFILING—APPLICATIONS AND SUBSCRIBERS

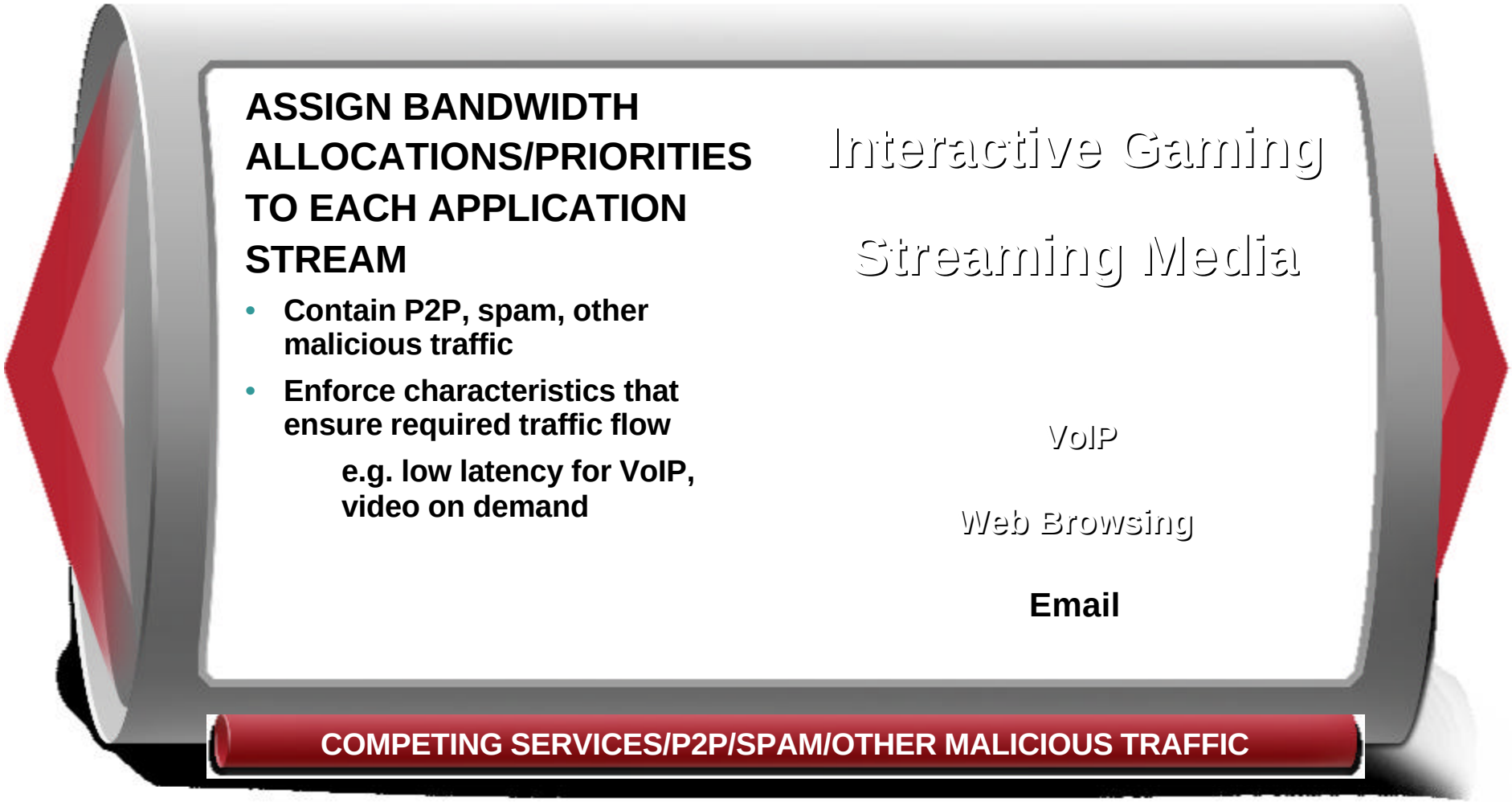


SUBSCRIBERS	APPLICATIONS
Telecommuters/SOHO	VPN, Browsing, VoIP, eMail
General Family Use (Daily Use of Internet)	Browsing, eMail, VoD
Children/In-Home Students (Heavy Use of Internet)	Browsing (eg. Disney), eMail, IM, P2P, Gaming
Occasional Users (Internet Used On Occasion)	Browsing, eMail
"As Required" Users (Internet Used Rarely)	eMail
Higher Ed Students	Browsing, Skype, eMail, IM, P2P, Gaming

Step 2: Service Optimization

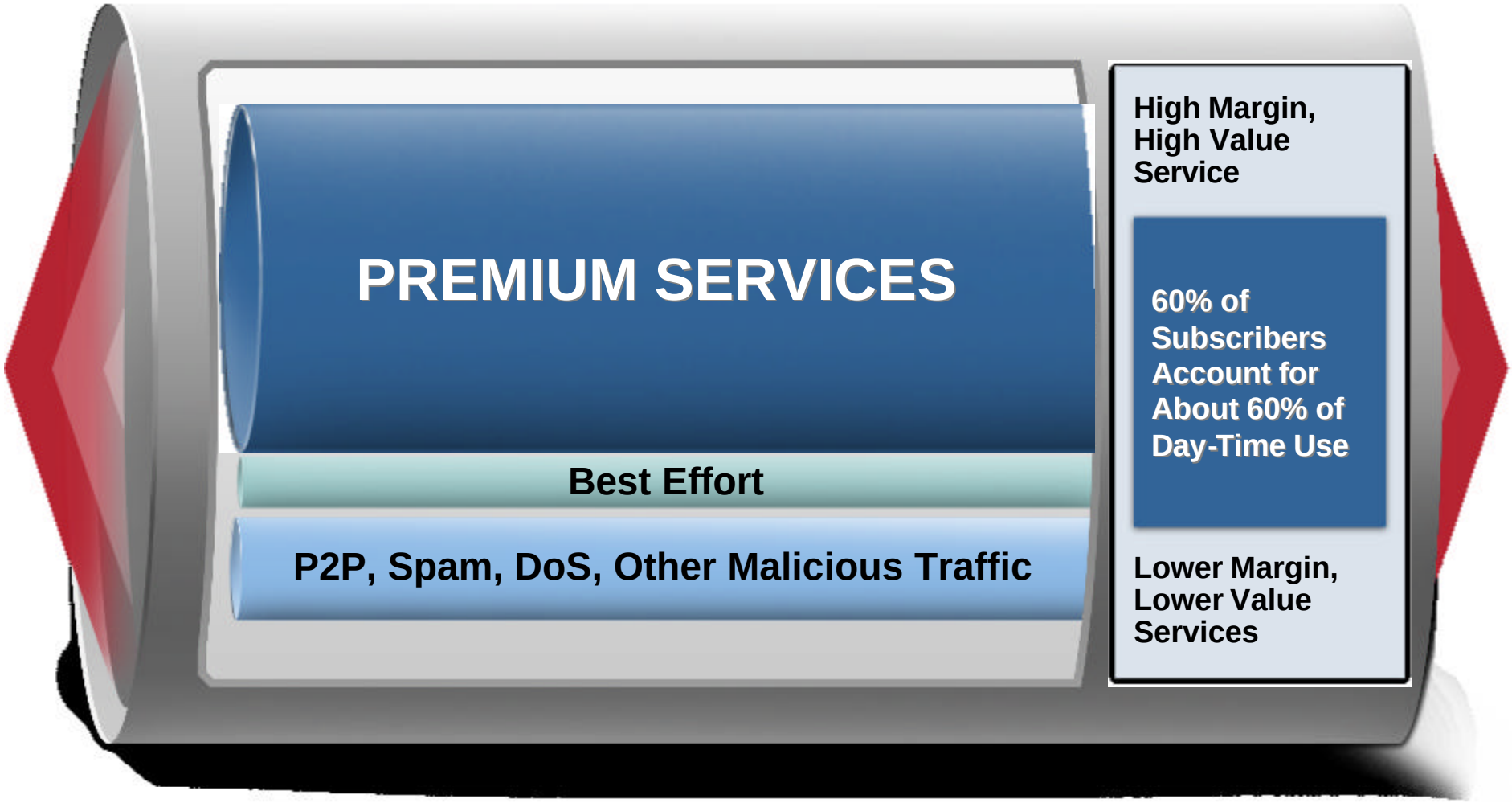
Cisco.com

"CONDITION" NETWORK TO CONFORM TO BUSINESS MODEL

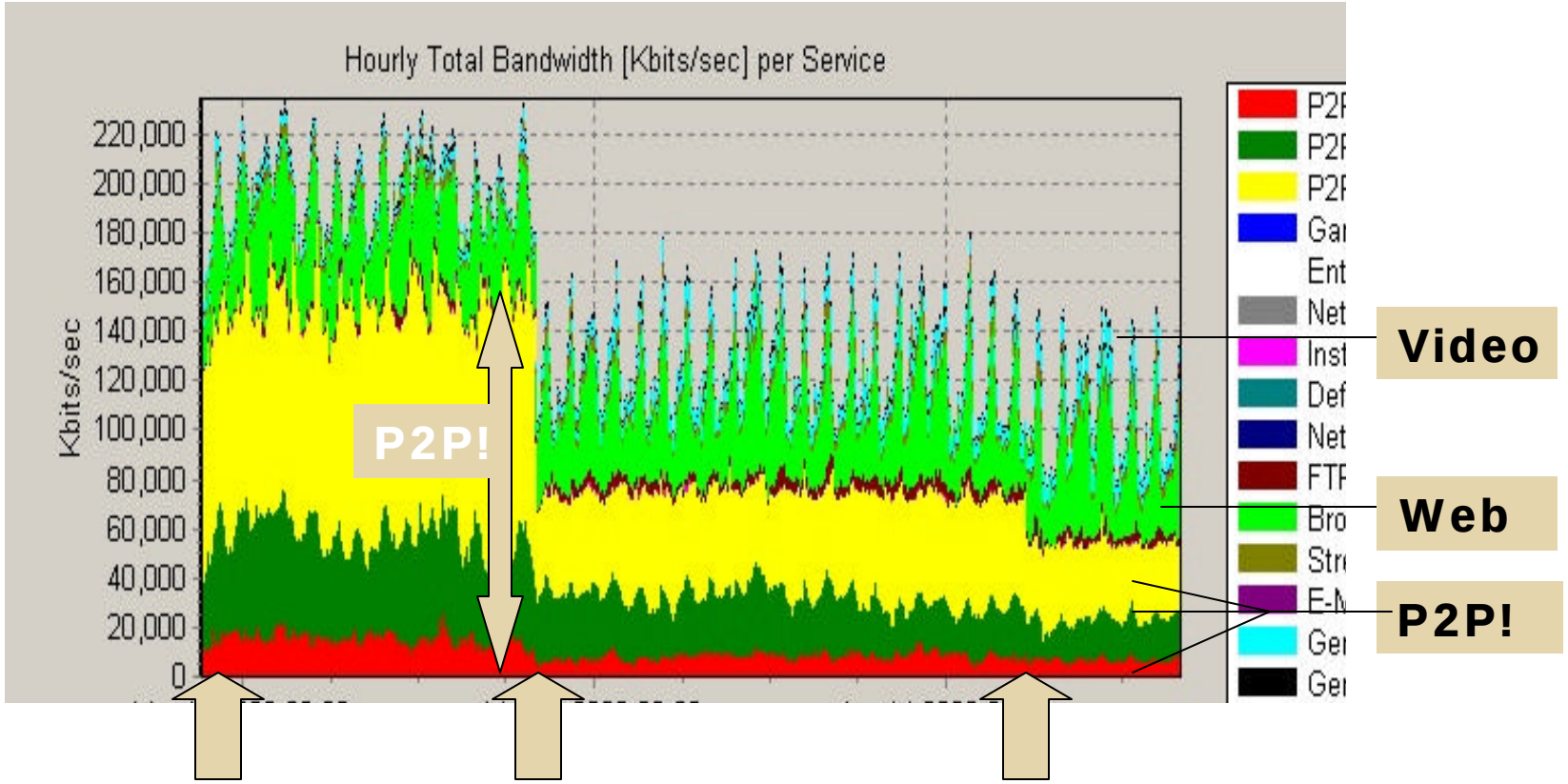


Step 3: Service Differentiation

DEFINE, ENFORCE, AND BILL FOR SERVICE OFFERINGS



Application Traffic Optimization (P2P, …)

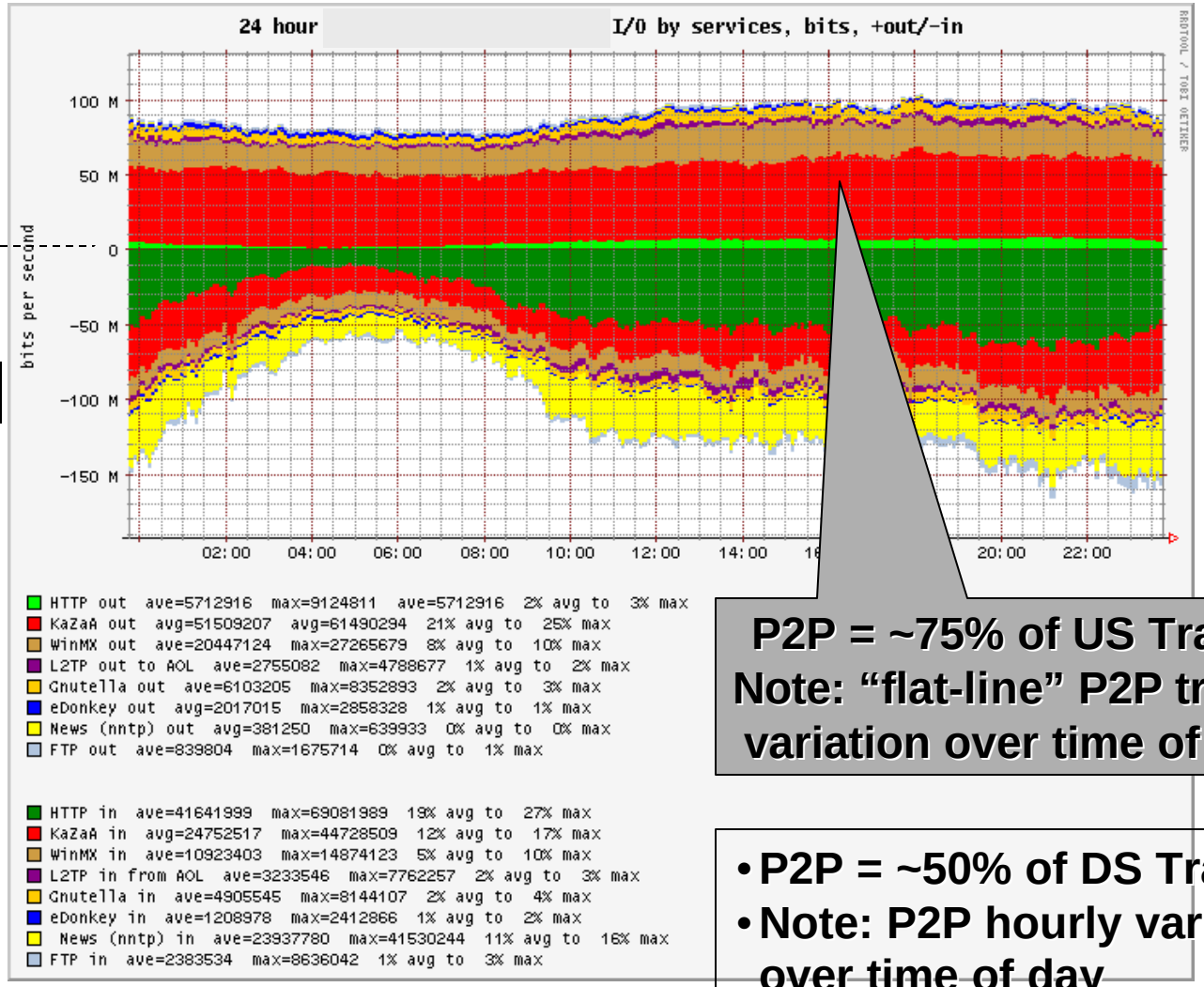


Number of support calls with complaints on level of service was reduced to zero!

What Subscribers are Doing:
24 Hour Aggregate Subscriber Traffic

Upstream Traffic

Downstream Traffic



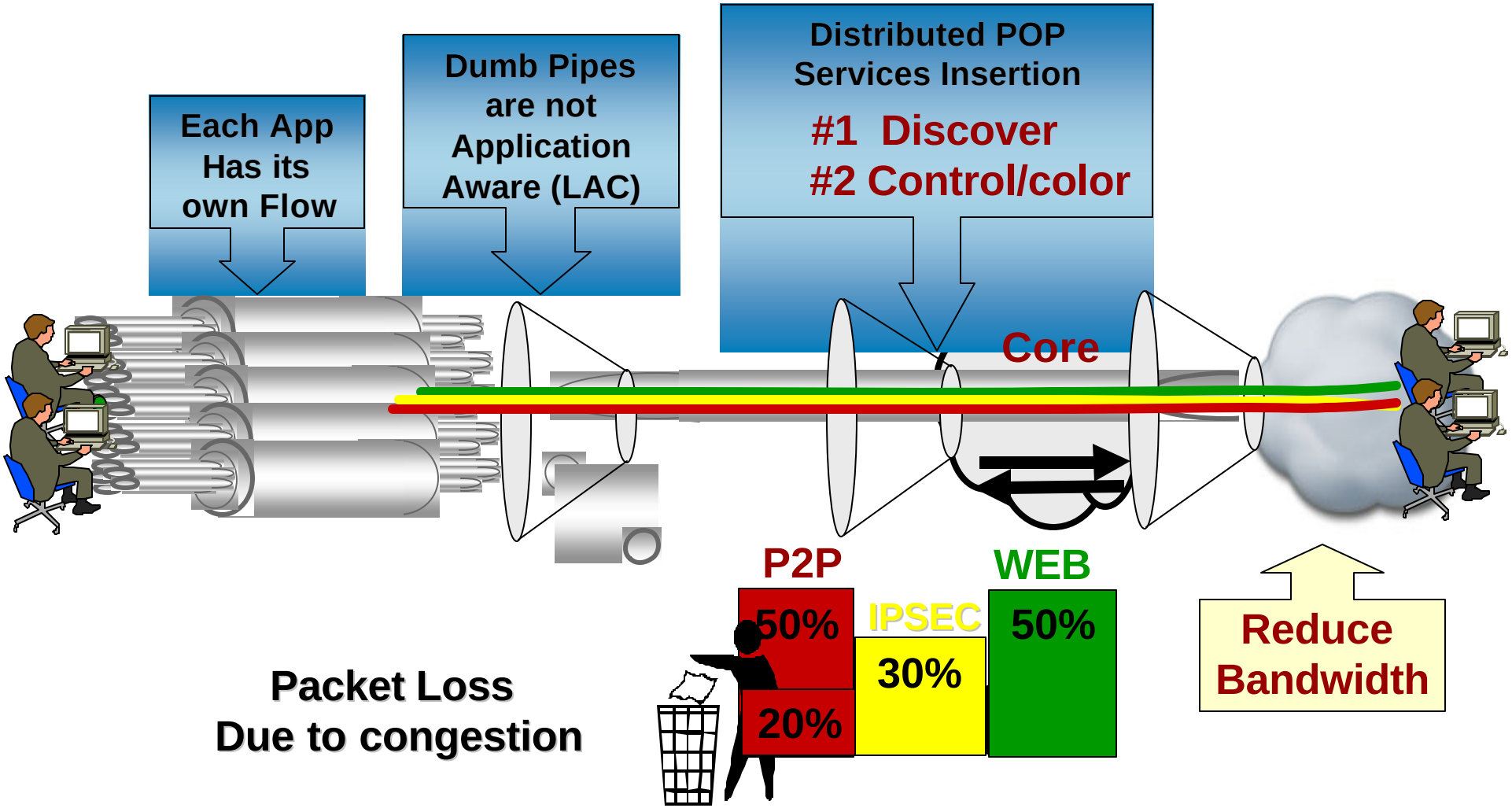
P2P = ~75% of US Traffic
Note: "flat-line" P2P traffic variation over time of day

- **P2P = ~50% of DS Traffic**
- **Note: P2P hourly variation over time of day**

Building Intelligent Pipes

Network Based Application Control or PCUBE

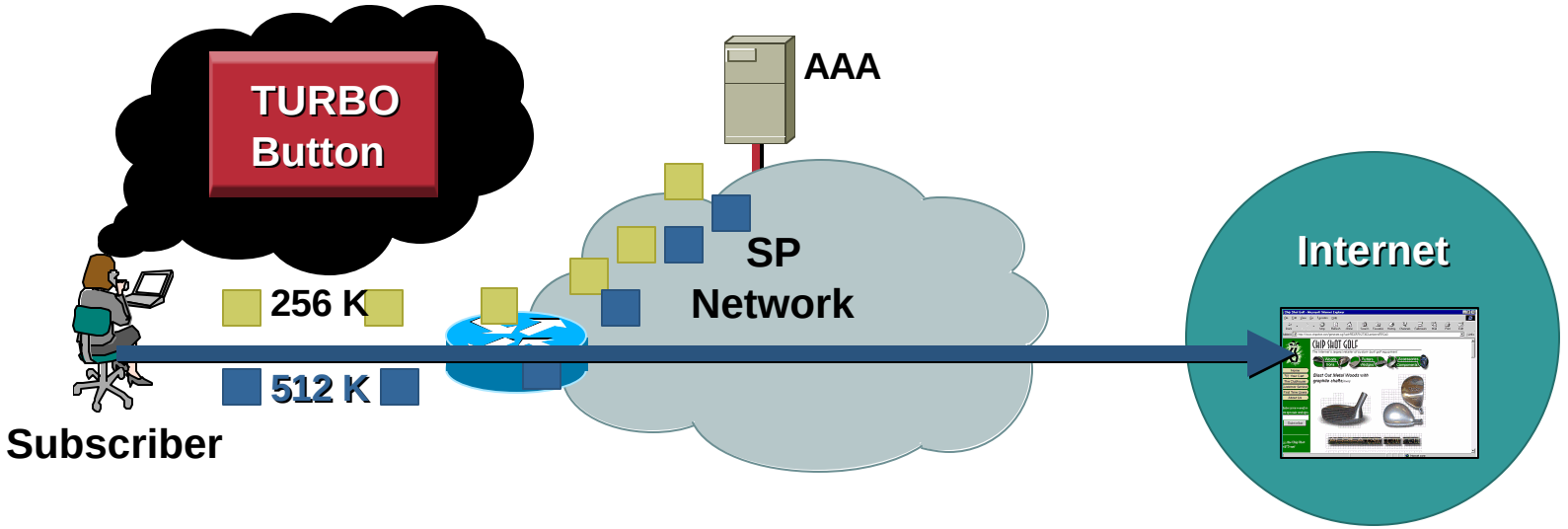
Cisco.com



Dynamic Bandwidth Selection (DBS)

- Allows subscribers to change bandwidth dynamically
- Generates AAA accounting records for billing
- Works by changing the ATM VC shaping parameters
- Helps subscriber:
  - Higher bandwidth for services that need it, when they need it
  - High bandwidth service (video) at lower overall subscription cost
- Helps service provider:
  - Offer financially attractive service to customers
  - Bill customers for high bandwidth usage

DBS—Basic Operation



- A subscriber's RADIUS user-profile contains ATM VC shaping rate
- User authentication (PPPoEoA or PPPoA):
  - Downloads the shaping rate (AAA authorization)
  - Changes subscriber's VC parameters accordingly
  - Supports UBR and VBR-nrt VCs
  - Doesn't delete and reinstall VC, or bring down PPP session
  - Layer two; hence no performance impact

DBS—Configuration—UBR VCs

Cisco.com

RADIUS Profile

```
john Password = "cisco"
        avpair="vpdn:tunnel-id=lac",
        avpair="vpdn:tunnel-type=l2tp",
        avpair="vpdn:l2tp-tunnel-password=lab",
        avpair="vpdn:ip-addresses=222.1.1.2",
        avpair="atm:peak-cell-rate=256000“
```

Router Configuration

```
interface atm0/0/0.1 multipoint
 ip address 10.0.0.0 255.255.255.0
 range pvc 1/32 1/8031
  dbs enable
```

DBS—Configuration—VBR VCs

Cisco.com

RADIUS Profile

```
John Password = "cisco"
        avpair="vpdn:tunnel-id=lac",
        avpair="vpdn:tunnel-type=l2tp",
        avpair="vpdn:l2tp-tunnel-password=lab",
        avpair="vpdn:ip-addresses=222.1.1.2",
        avpair="atm:peak-cell-rate=256000“
        avpair=“atm:sustainable-cell-rate=256000”
```

Router Configuration

```
interface atm0/0/0.1 multipoint
 ip address 10.0.0.0 255.255.255.0
 range pvc 0/50 0/70
  vbr-nrt 5000 50
  dbs enable
```

DBS Configuration Options

Configuration on VC

```
interface ATM0/0/0.5 point-to-point
 ip address 172.1.2.3
 pvc 0/100
  dbs enable
  protocol pppoe
```

Configuration on VC Range

```
interface ATM0/0/0.1 multipoint
 ip address 172.1.2.3
 range pvc 0/50 0/70
  dbs enable
```

Configuration on VC Class

```
vc-class atm pppoe
   dbs enable
```

Configuration with PVC-in-Range

```
interface ATM0/0/0.1 multipoint
range pvc 0/50 0/70
pvc-in-range 60
dbs enable
```

Configuration with VC Class Inheritance

```
vc-class atm pppoe
dbs enable

interface ATM0/0/0.5 point-to-point
pvc 0/90
no dbs enable
vbr-nrt 5000 50
class-vc pppoe
protocol pppoe
```

DBS Configuration Options

1. No sessions on a VC => PCR/SCR configured for VC by CLI is used
2. When a session with DBS comes up, the VC's SCR/PCR are modified per DBS
   - RADIUS parameters have precedence over CLI
   - After all PPPoX sessions on a VC die, PCR/SCR configured by CLI take effect
3. For VC with multiple PPPoE sessions:
   - Max SCR/PCR among all sessions are applied to VC
   - When session with max PCR/SCR dies, next highest PCR/SCR is used

DBS—Accounting Records

QoS values applied by DBS for a particular user will be sent to the AAA server in START/STOP accounting record for that user.

Accounting attributes in a typical record looks like this.
Cisco-Avpair = "peak-cell-rate=155000" [flags = 0x00014000]
Cisco-Avpair = "sustainable-cell-rate=145000" [flags = 0x00014000]

DBS—Verification

Cisco.com

```
dbs# show atm pvc dbs
VCD / Peak Avg/Min Burst
Interface Name VPI VCI Type  Encaps  SC    Kbps Kbps Cells   Sts
1/0.7       3    1   95  PVC  MUX     VBR  2000  700   94    UP
```

More Information on DBS At:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftdbs.htm

Quality of Service

Cisco.com

- QoS—major infrastructure for differentiated service
  - Layer 2 QoS: ATM service class, DBS
    - Hardware assisted—no performance impact
    - Per subscriber (per VC) differentiation (not per-session)
  - Layer 3 QoS
    - Hardware assist—platform specific
    - Per session/per subscriber QoS—better flexibility
      - Major QoS features for Broadband
      - Classification
      - Policing
      - Marking
      - Queuing

IP Policing

Most Deployed IP Qos Feature in Broadband

1. **Policing rate-limits traffic to specified rate (kbps)**
   - **Does not buffer exceeding packets (simply drops)**
2. **Shaping is similar, but:**
   - **It buffers exceeding traffic**
   - **Drops packets only when buffer is full**
   - **Uses more CPU resource (Vs. policing) due to buffering**
3. **IP policing is OK for rate-limiting Internet access**
   - **Policing shouldn't drop loss/delay-sensitive traffic (e.g., voice)**

IP Policing—INET Access

Cisco.com

1. **Service providers have successfully deployed policing for INET access (tiered service)**
   - **For bandwidth differentiated tiered service**
   - **Allows uniform ATM provisioning across tiers**
2. **Downstream traffic policing typical (upstream possible)**
3. **Policing parameter options:**
   1. **Downloaded from radius**
   2. **Locally defined in virtual template**

IP Policing— CAR Versus MQC Policing

Cisco.com

Committed Access Rate (CAR)

- Older feature
- Can be applied on
  - Interface,
  - Virtual template
- Works with CEF only
- Can ‘mark’ with IP precedence

Modular QoS CLI (MQC) Policing

- Newer Feature
- Can be applied on
  - Interface
  - Virtual template
  - VC
- Works with CEF,fast, process
- Marks with IP precedence or DSCP
- All future QoS development on MQC

MQC Policing—Local Configuration

- **Local per-session policing configuration**
  - **Configured on the virtual template**
  - **Uses globally defined QoS policy**
- **Simplest config: use class-default (don't define specific classes unless needed)**

```
policy-map isp1-policy          // defines a policy map
  class class-default           // all traffic matches this class
    police 256000 32000 64000 conform-action transmit exceed-action drop
 !
                                // 32000 = burst size, 64000= excess burst size
interface Virtual-Template1
 ppp authentication chap
 ....
 service-policy output isp1-policy   // applies QoS policy above to each VA
                                        interface cloned
```

MQC Policing— Traditional AAA Download

- Policing parameters downloaded via lcp:interface-config AV pair
- Only service-policy command is downloaded, the policy itself should be defined in router config

"virtual-profile AAA" Command is NOT Necessary

```
policy-map isp1-policy
  class class-default            // all traffic matches this class
    police 256000 32000 64000 conform-action transmit exceed-action drop
 !
// 32000 = burst size, 64000 = excess burst size
interface Virtual-Template1
  ppp authentication chap
  ....
```

Affects Ppp Call Rate Due to Parsing of Downloaded Command String

No Spaces Before/after =

```
Radius User Profile:
User1   Password = "cisco"
        Service-Type = Framed,
        Framed-Protocol = PPP,
        Framed-MTU = 1500,
        Cisco-Avpair = "lcp:interface-config=service-policy output isp1-policy"
```

MQC Policing— New Download Configuration

To improve PPP call rate, 12.2(15)B introduces two new cisco VSA's:

- **Cisco VSA type 37 -> Upstream policy for subscriber**
- **Cisco VSA type 38 -> Downstream policy for subscriber**

For Merit server, in dictionary following lines need to be added

```
Cisco.attr      Cisco-Policy-Up          37      string (*, *)
Cisco.attr      Cisco-Policy-Down        38      string (*, *)
```

Radius user profile specifies the policyname & whether up/downstream

```
username    Password = "cisco"
       Service-Type = Framed,
       Framed-Protocol = PPP,
       Cisco:Cisco-Policy-Down =“isp1-policy“
```

Policies themselves are defined in router config,

```
policy-map isp1-policy
  class class-default              // all traffic matches this class
    police 256000 16000 32000 conform-action transmit exceed-action drop
```

Quality of Service—Queuing Configuration


```
class-map match-any voip
  match ip precedence 5
class-map match-any video
  match ip precedence 4
!
!
policy-map cbwfq_out_policy
  class voip
    priority 64
  class video
    bandwidth 3500
  class class-default
    bandwidth 128
```

```
interface ATM2/0/0.81833 point-to-point
 pvc 81/833
  vbr-nrt 7680 7680 32
  encapsulation aal5snap
  pppoe max-sessions 1
  service-policy output cbwfq_out_policy
  protocol pppoe
 !
!
interface ATM2/0/0.81834 point-to-point
 pvc 81/834
  vbr-nrt 7680 7680 32
  encapsulation aal5snap
  pppoe max-sessions 1
  service-policy output cbwfq_out_policy
  protocol pppoe
```

Quality of Service—Performance Impact

- **Platforms with hardware assisted QoS: little performance impact**

  E.g.: c10K: per session policing on 61500 sessions, with 8 OC-3 ports—no throughput impact with policing vs. without

- **Platforms without hardware assisted QoS: Performance impacted by CPU usage (memory usage is low)**

  MQC Policing~30% throughput impact

  CAR Policing~20–25% throughput impact

  Note: One way policing, no ACL classification

  CBWFQ—Higher impact due to queuing overhead

  —Depends on # of queues and other factors

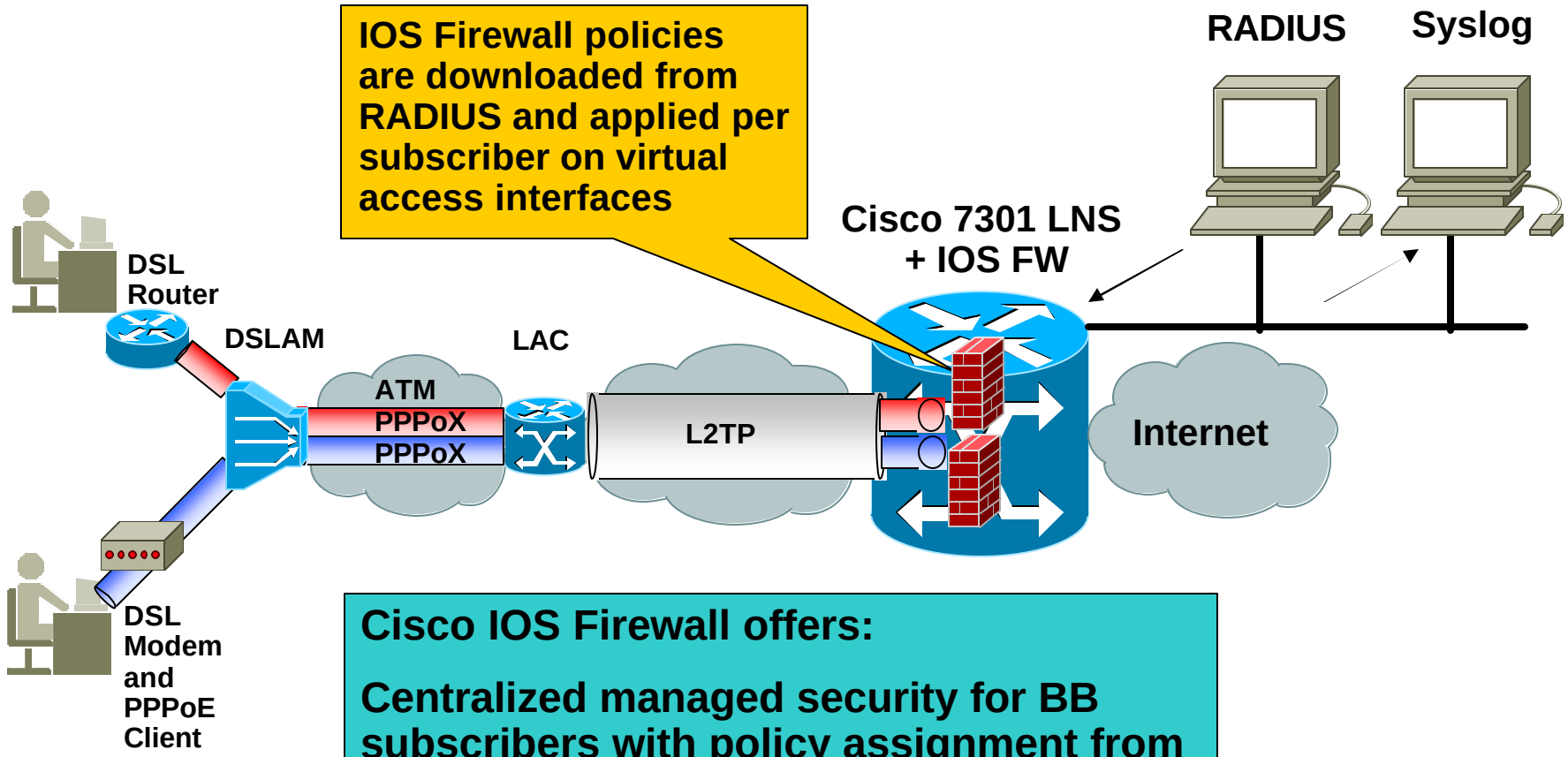
Service Infrastructure—Per Subscriber Security Services

- Per user security can be achieved via
  - Per user firewall
  - Unicast RPF
- Configured in RADIUS-user profile—simplifies subscriber provisioning
- Can be provided by SP bundled with services

Per User Firewall for BBA

- Provides security for Broadband subscribers
- Can be deployed as mass market service
- Provides application level monitoring at a session level, stateful packet inspection
- Is implemented on a per subscriber basis and thus can be individualized (to some degree)
- Provides easy firewall assignment to users via RADIUS
- Is centrally managed as opposed to personal FW and CPEs
- Is based on Cisco IOS Firewall

Cisco IOS Firewall for DSL Broadband subscribers

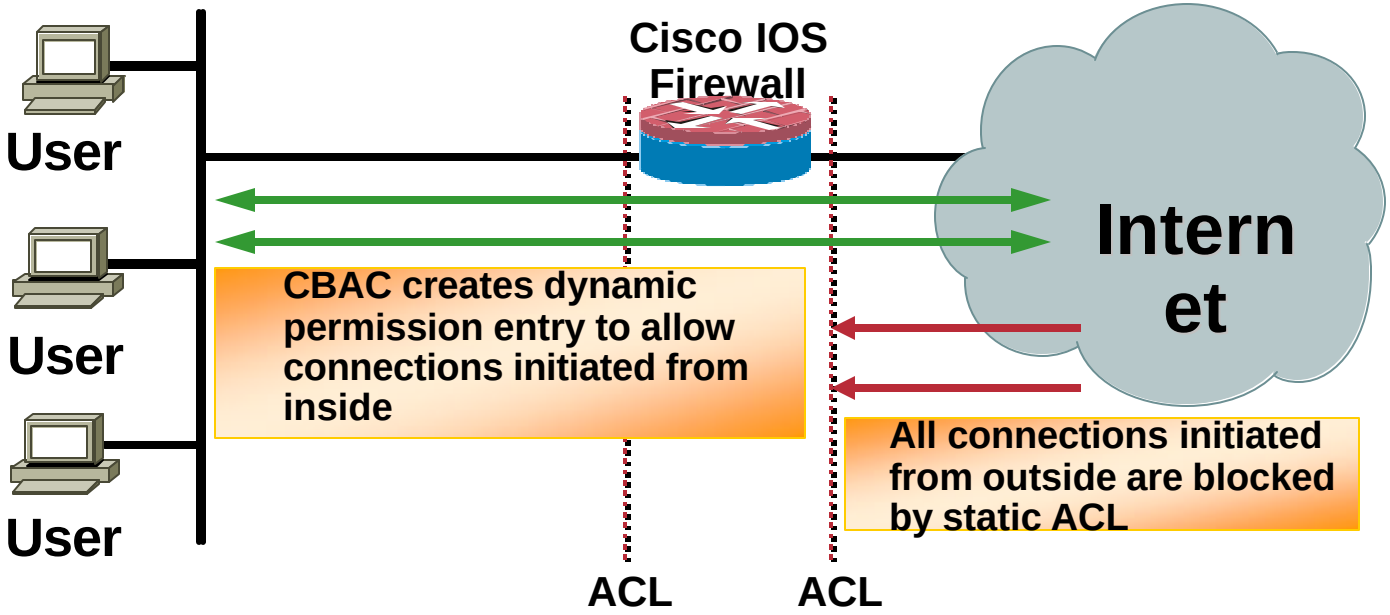


Cisco IOS Firewall offers:

Centralized managed security for BB subscribers with policy assignment from RADIUS and per user logging to Syslog

Subscribers are firewalled between each other and towards the Internet

Cisco IOS Firewall a.k.a. Context-Based Access Control (CBAC)



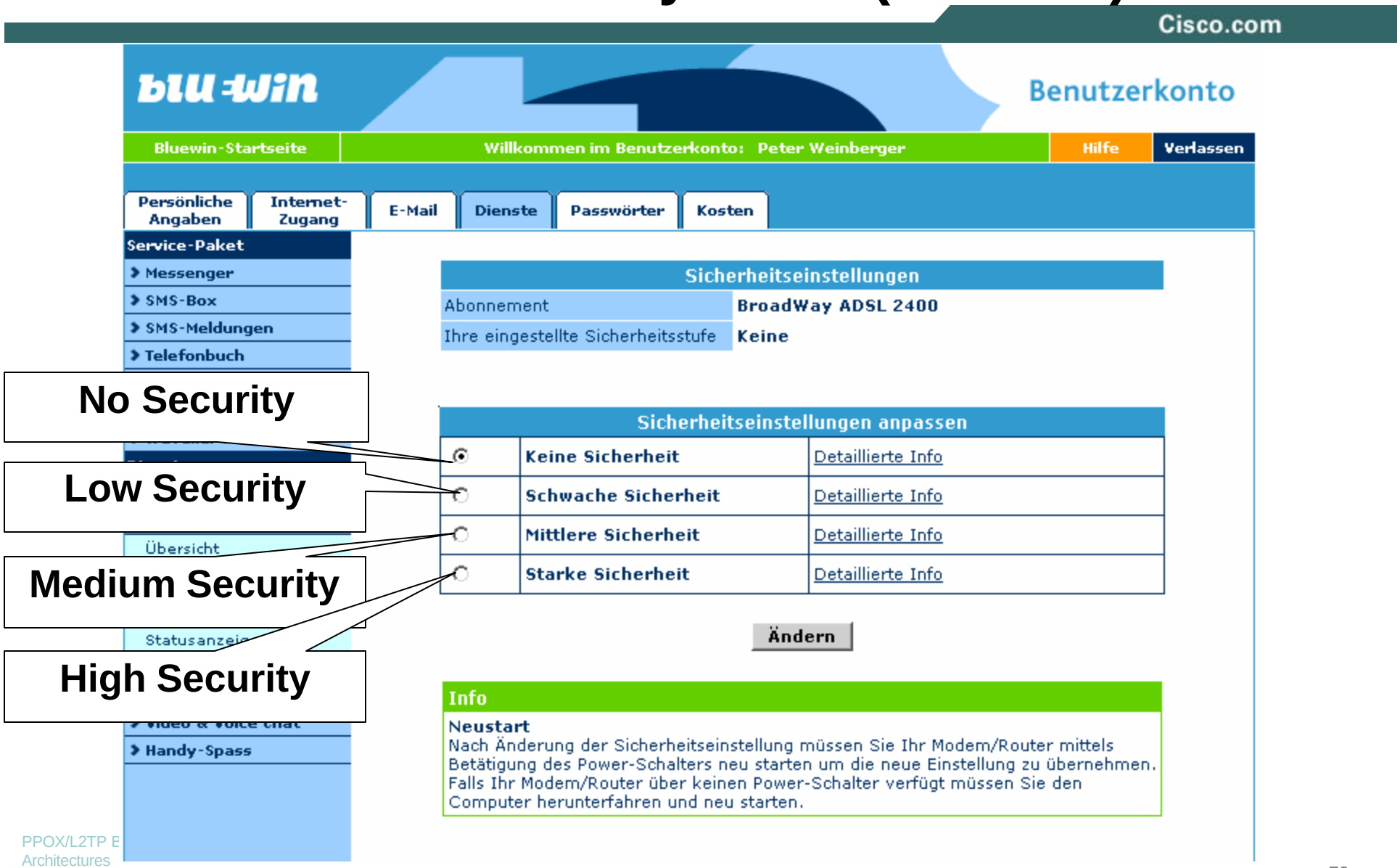
- Packet inspection system based on connection states and payload
- Uses dynamic access-lists
- Works with IPSec and NAT
- Provides DOS prevention capabilities
- Intercepts the packet after ACL check and routing setup
- For traffic passing through the router, not destined for it

Security Levels

A Security level or policy is build from two functions:

1. **ACL**
   - **An ACL defines which protocols should be allowed to transit IOS firewall**
   - **All capabilities of an extended ACL in IOS can be used**
   - **An ACL in and outbound can be downloaded from RADIUS at PPP session authorization**
2. **IOS Firewall Inspection rules**
   - **A CBAC inspection rule specifies what IP traffic (which application-layer protocols) will be inspected by CBAC at an interface.**
   - **An inspection rule should specify each desired application-layer protocol as well as generic TCP or generic UDP if desired. The inspection rule consists of a series of statements each listing a protocol and specifying the same inspection rule name.**

Selection of Security Level (German)



Per User Firewall – Configuration (1) ACL

Cisco AVpair [1] 33 "ip:inacl=100"

Local configuration on the LNS:

```
access-list 100 remark “lowsec"
access-list 100 permit tcp any any
access-list 100 permit udp any any
access-list 100 permit icmp any any
access-list 100 deny   ip any any log
```

This ACL defines which traffic is allowed to come FROM the subscriber.

Per User Firewall – Configuration (2) ACL


```
Cisco AVpair [1] 33 "ip:outacl#1=deny ip
any any log"
```

This ACL blocks by default all traffic coming from OUTSIDE unless it is allowed by CBAC.

Per User Firewall – Configuration (3) CBAC


```
Cisco AVpair [1] 48 "lcp:interface-
config#=ip inspect lowsec in"
```

Local configuration on the LNS:

```
ip inspect name lowsec tcp
ip inspect name lowsec udp
ip inspect name lowsec icmp
```

This command causes CBAC to inspect the packets coming into this interface from the network. If a packet is attempting to initiate a session, CBAC will then determine if this protocol is allowed, create a CBAC session, add the appropriate ACLs to allow return traffic and do any needed content inspection on any future packets for this session.

Per User Firewall – Configuration (4) CBAC global


```
ip inspect max-incomplete high 60000
ip inspect max-incomplete low 60000
ip inspect one-minute high 120000
ip inspect one-minute low 60000
ip inspect hashtable-size 8192
ip inspect tcp max-incomplete host 10000
block-time 2
```

Per User Firewall – show commands (1) “show ip inspect all”

Cisco.com

```
peweinbe#sh ip inspect all
Session audit trail is disabled
Session alert is enabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name myfw
    fragment Maximum 256  In Use 0 alert is on audit-trail is off timeout 1
    ftp alert is on audit-trail is off timeout 3600
    h323 alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
    realaudio alert is on audit-trail is off timeout 3600
    rtsp alert is on audit-trail is off timeout 3600
    sip alert is on audit-trail is off timeout 30
    skinny alert is on audit-trail is off timeout 3600
    sqlnet alert is on audit-trail is off timeout 3600
    streamworks alert is on audit-trail is off timeout 30
    tcp alert is on audit-trail is off timeout 3600
    tftp alert is on audit-trail is off timeout 30
    udp alert is on audit-trail is off timeout 30
    vdolive alert is on audit-trail is off timeout 3600
```

Per User Firewall – show commands (2) “show ip inspect all”

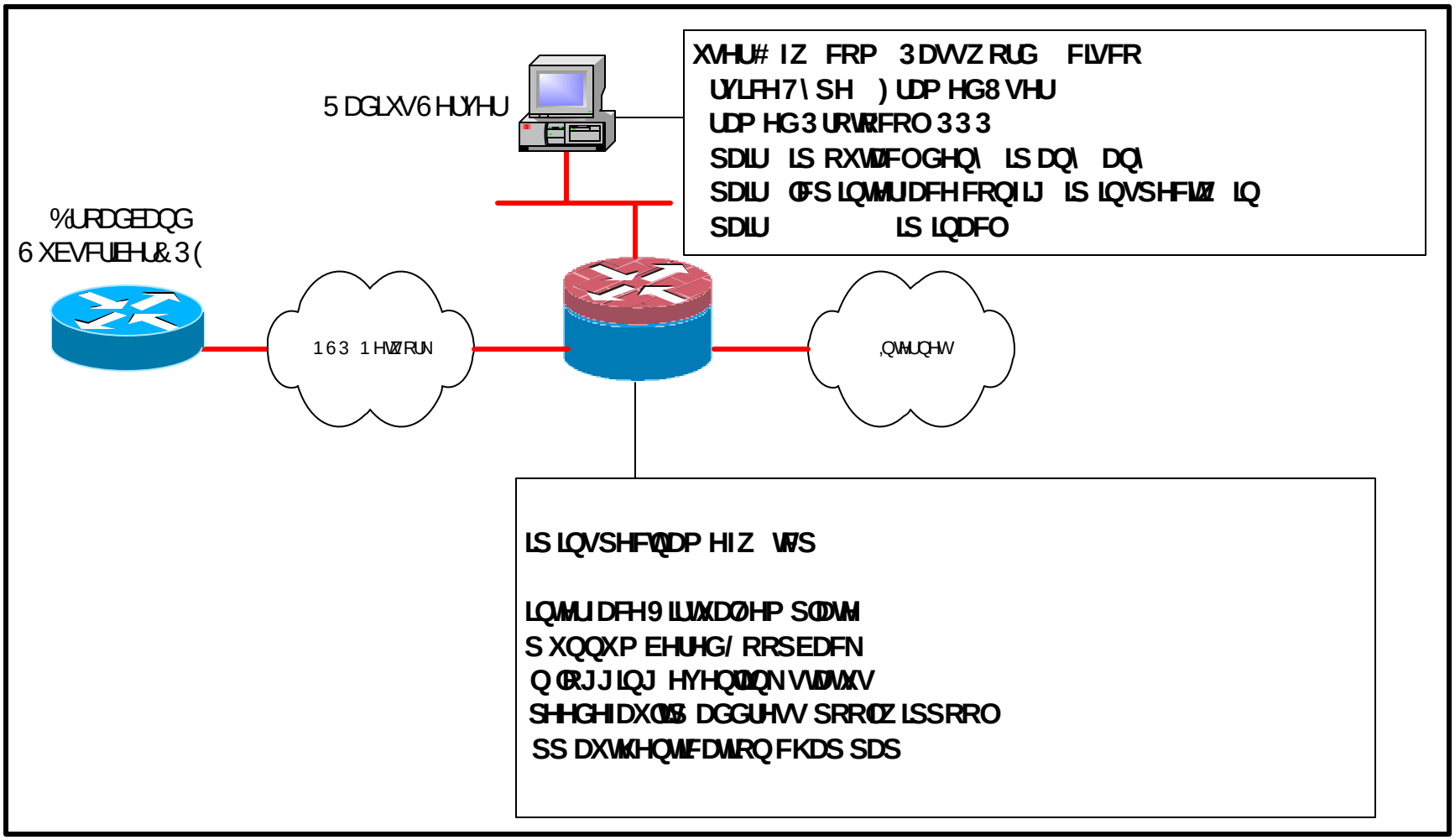

```
Interface Configuration
 Interface FastEthernet0/0
  Inbound inspection rule is myfw
    fragment Maximum 256  In Use 0 alert is on audit-trail is off timeout 1
    ftp alert is on audit-trail is off timeout 3600
    h323 alert is on audit-trail is off timeout 3600
    http alert is on audit-trail is off timeout 3600
    icmp alert is on audit-trail is off timeout 10
    realaudio alert is on audit-trail is off timeout 3600
    rtsp alert is on audit-trail is off timeout 3600
    sip alert is on audit-trail is off timeout 30
    skinny alert is on audit-trail is off timeout 3600
    sqlnet alert is on audit-trail is off timeout 3600
    streamworks alert is on audit-trail is off timeout 30
    tcp alert is on audit-trail is off timeout 3600
    tftp alert is on audit-trail is off timeout 30
    udp alert is on audit-trail is off timeout 30
    vdolive alert is on audit-trail is off timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is 100
  Outgoing access list is 101

Half-open Sessions
 Session 83F822A4 (172.16.0.6:3652)=>(144.254.208.7:1029) udp SIS_OPENING
 Session 83F747CC (172.16.0.6:3654)=>(10.51.84.6:2748) tcp SIS_OPENING
 Session 83F8185C (172.16.0.6:3652)=>(171.70.156.233:1029) udp SIS_OPENING
 Session 83F77844 (172.16.0.6:3651)=>(171.71.179.243:1533) tcp SIS_OPENING
 Session 83F7CA84 (172.16.0.6:3652)=>(144.254.74.56:1029) udp SIS_OPENING
 Session 83F76994 (172.16.0.6:3653)=>(171.70.156.233:1029) tcp SIS_OPENING
 Session 83F7681C (172.16.0.6:137)=>(144.254.229.98:137) udp SIS_OPENING
 Session 83F83444 (172.16.0.6:3652)=>(144.254.6.144:1029) udp SIS_OPENING
```

Per User Firewall – show commands (3) “show ip inspect sessions”

Cisco.com

```
peweinbe#sh ip inspect sessions detail
Half-open Sessions
 Session 83F7681C (172.16.0.6:137)=>(64.103.102.42:137) udp SIS_OPENING
  Created 00:00:00, Last heard 00:00:00
  Bytes sent (initiator:responder) [68:0]
  Out SID 64.103.102.42[137:137]=>172.16.0.6[137:137] on ACL 101
 Session 83F747CC (172.16.0.6:3720)=>(10.51.84.5:2748) tcp SIS_OPENING
  Created 00:00:06, Last heard 00:00:03
  Bytes sent (initiator:responder) [0:0]
  Out SID 10.51.84.5[2748:2748]=>172.16.0.6[3720:3720] on ACL 101
 Session 83F77844 (172.16.0.6:3718)=>(144.254.208.7:1029) udp SIS_OPENING
  Created 00:00:23, Last heard 00:00:23
  Bytes sent (initiator:responder) [0:0]
  Out SID 144.254.208.7[1029:1029]=>172.16.0.6[3718:3718] on ACL 101
 Session 83F7CA84 (172.16.0.6:3718)=>(144.254.74.56:1029) udp SIS_OPENING
  Created 00:00:23, Last heard 00:00:23
  Bytes sent (initiator:responder) [0:0]
  Out SID 144.254.74.56[1029:1029]=>172.16.0.6[3718:3718] on ACL 101
 Session 83F832CC (172.16.0.6:3719)=>(171.70.156.233:1029) tcp SIS_OPENING
  Created 00:00:18, Last heard 00:00:09
  Bytes sent (initiator:responder) [0:0]
  Out SID 171.70.156.233[1029:1029]=>172.16.0.6[3719:3719] on ACL 101
 Session 83F78114 (172.16.0.6:3718)=>(171.70.156.233:1029) udp SIS_OPENING
  Created 00:00:23, Last heard 00:00:23
  Bytes sent (initiator:responder) [0:0]
  Out SID 171.70.156.233[1029:1029]=>172.16.0.6[3718:3718] on ACL 101
```

Per User Firewall – Sample configuration Overview



Logging and Statistics – Requirements –

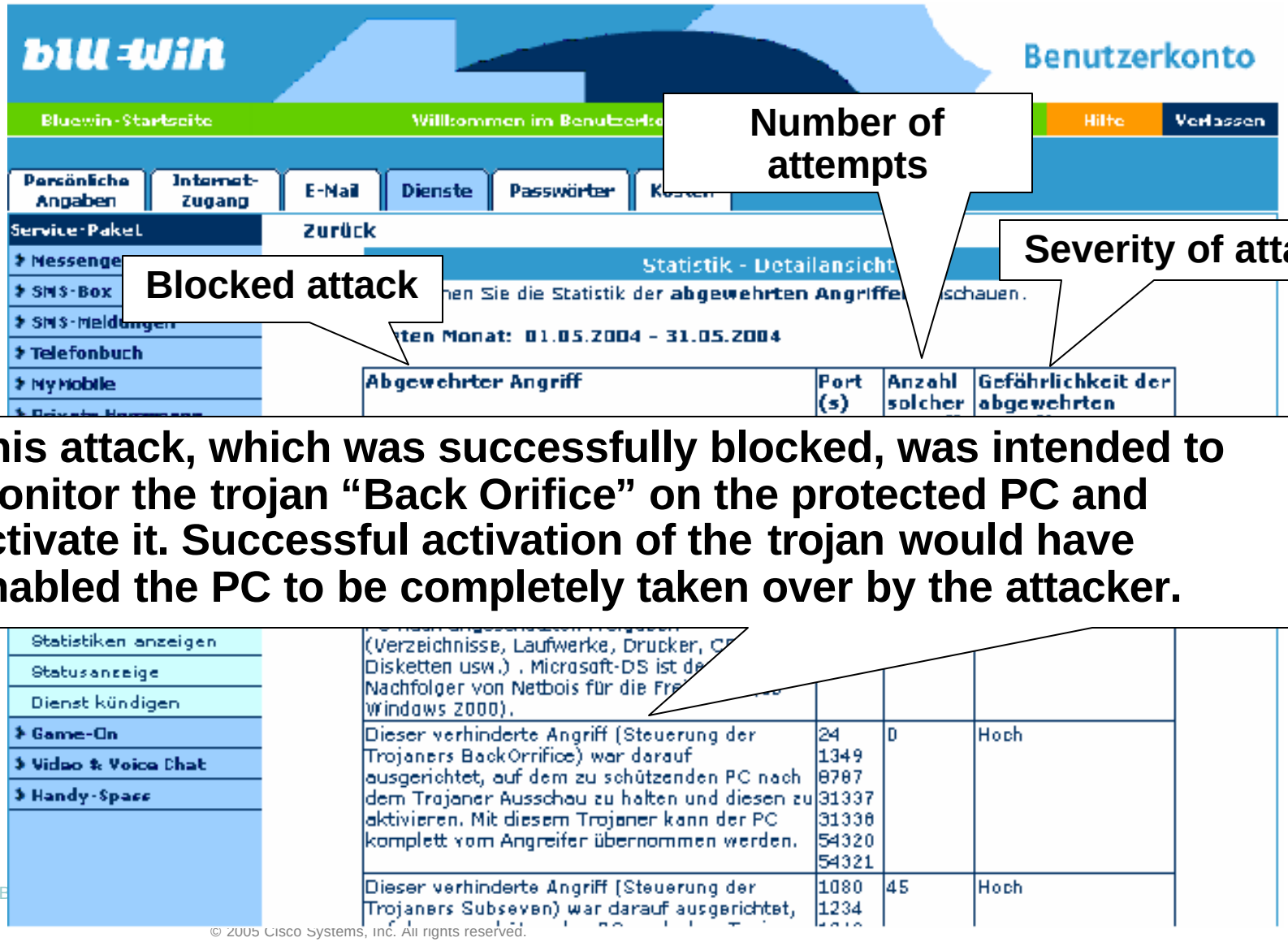
- Logging of unauthorized attempts to get access to users VAI
- ACL logging are correlated with IP address assignments from PPP/IPCP
- Consolidated data needs be presented to end-users in an understandable format
  - Explain what an logged event could mean
  - Explain well-known attacks

Logging and Statistics

- **ACL logging :**

Jun 20 01:15:42.308: %SEC-6-IPACCESSLOGRP: list 101 denied igmp 213.3.80.1 -> 10.0.0.11 (user@cisco.com, Interface Virtual-Access1.1, Inbound inspection rule is fwr-1), 1 packet

Statistics (German)



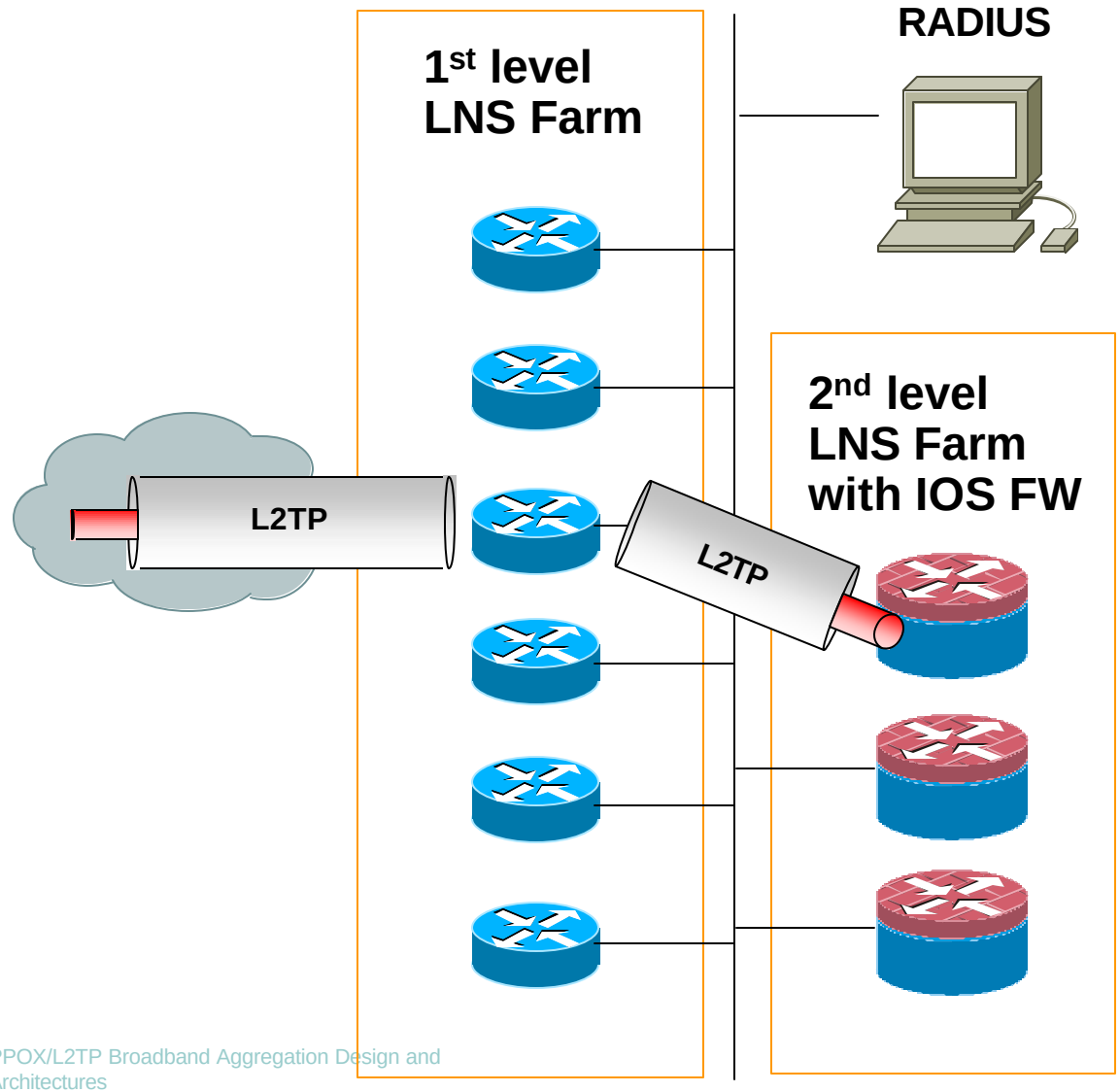
Number of attempts

Severity of attack

Blocked attack

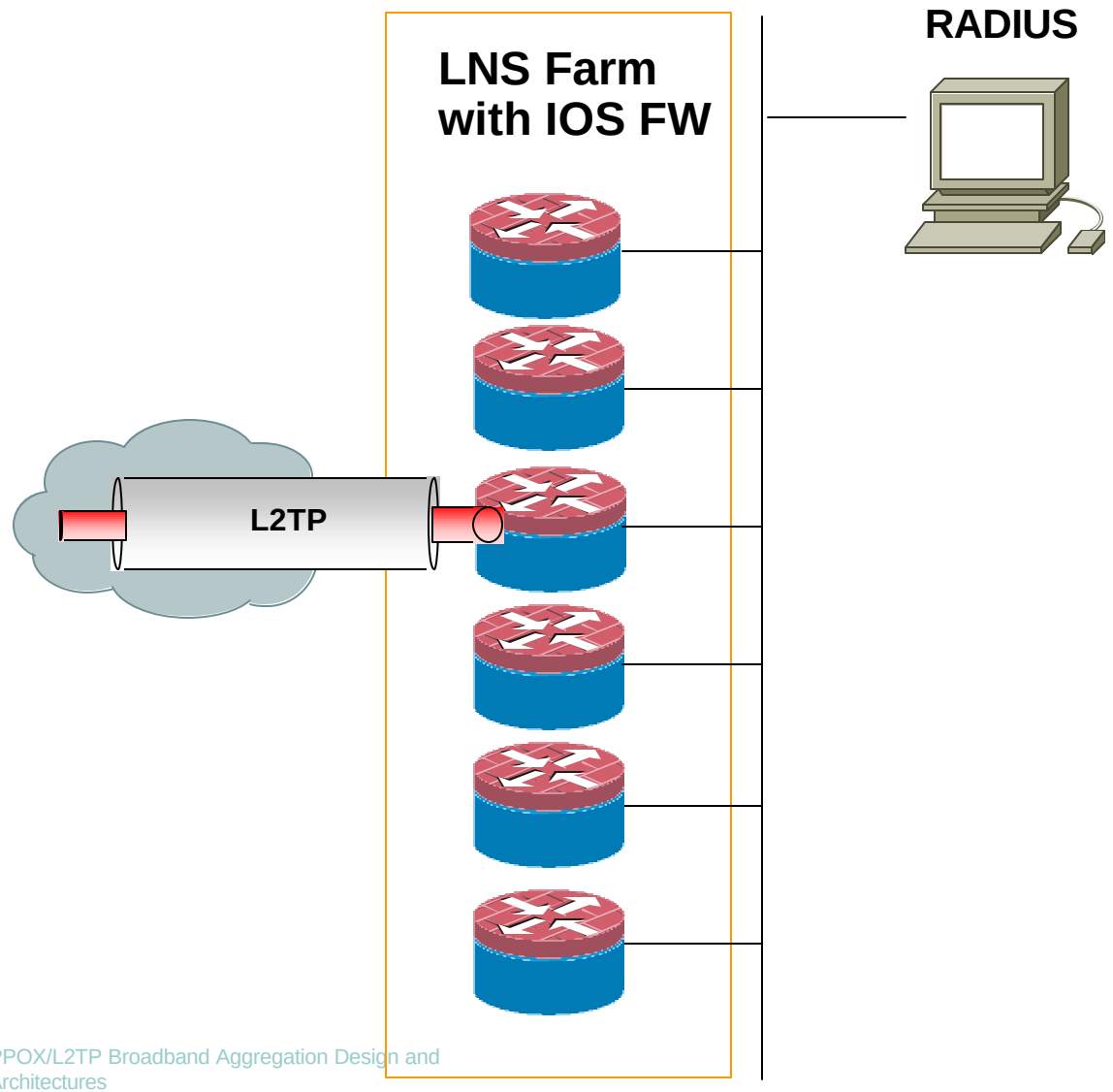
This attack, which was successfully blocked, was intended to monitor the trojan “Back Orifice” on the protected PC and activate it. Successful activation of the trojan would have enabled the PC to be completely taken over by the attacker.

Deployment Scenarios
(1) Dedicated Farm



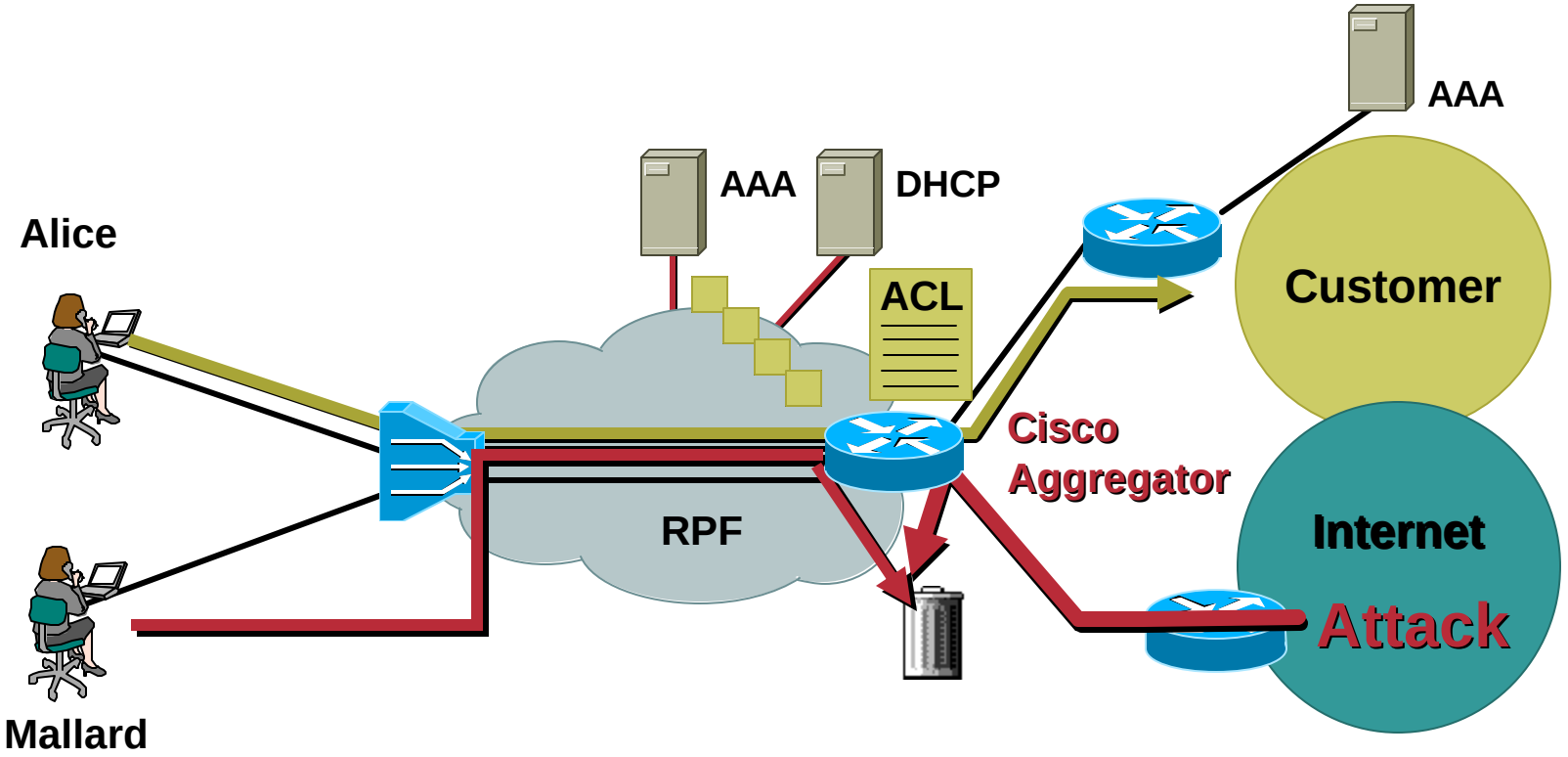
- Users subscribed for the firewall service are tunnel-switched from 1st level to 2nd level farm
- Per-user or by specific domain-name
- Dedicated farm could be operated by different team
- Useful if 1st level gear does not support per user FW

Deployment Scenarios (2) Firewall on all



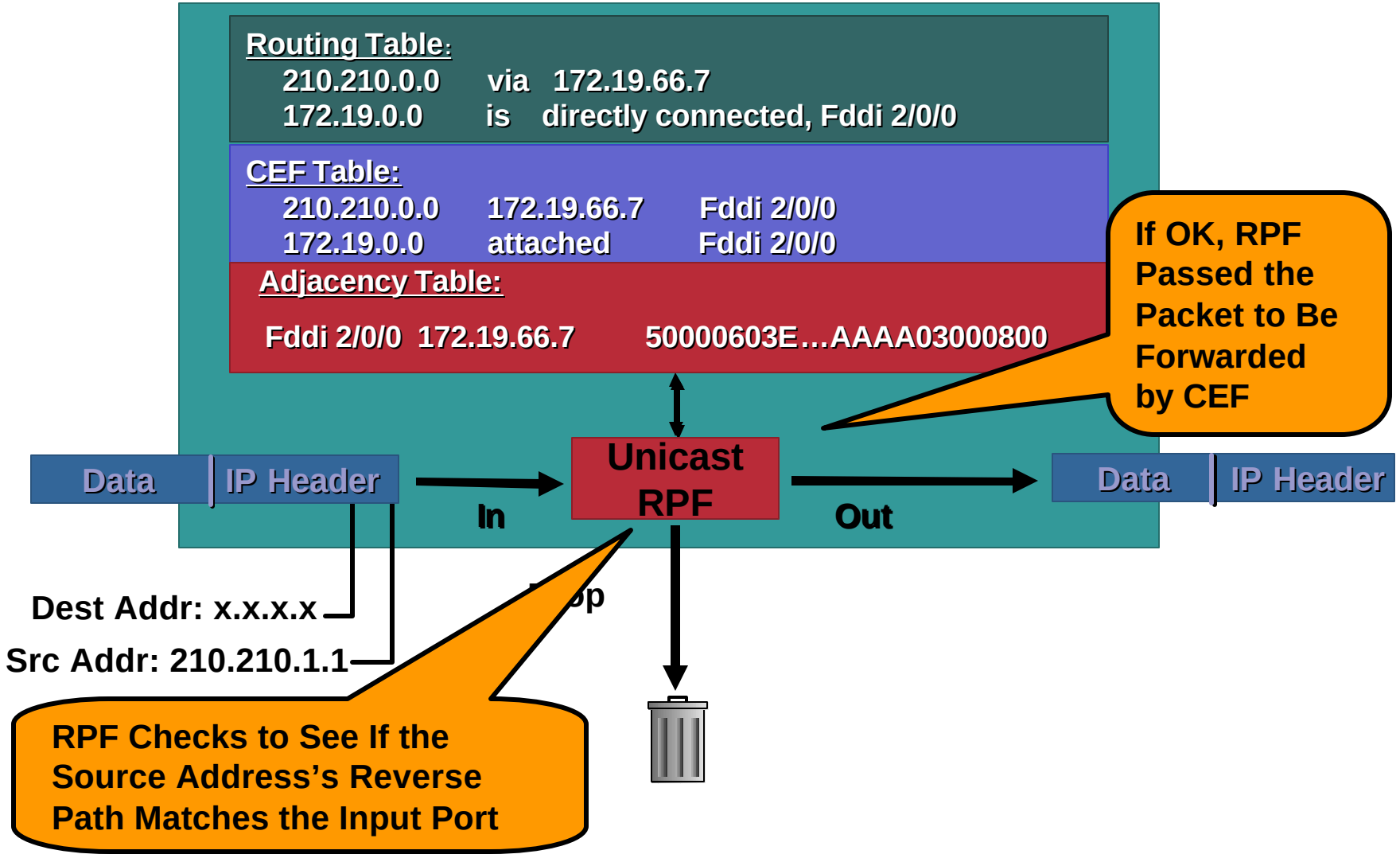
- Users are/should be equally distributed among all LNSs
- Consider BB FW site license rather than IOS FW license per box

Unicast Reverse Path Forwarding—uRPF



- Verify source IP address to prevent DoS attacks
- Protects subscribers and also Internet

Unicast Reverse Path Forwarding—uRPF



uRPF—Configuration

Cisco.com

```
interface ATM1/0/1.1 multipoint
 range pvc 2/32 2/65
  encapsulation aal5autoppp Virtual-Template1
 !
!
interface Virtual-Template1
 ip unnumbered Loopback0
 peer default ip address pool pool1
 ppp authentication chap
 ip verify unicast source reachable-via rx
!
```

RPFC—Verification


```
Router-3# show cef interface serial 2/0/0
Serial2/0/0 is up (if_number 8)
  Internet address is 192.168.10.2/30
  Per packet loadbalancing is disabled
  IP unicast RPF check is enabled

Router# show ip traffic
…
Drop:  3 encapsulation failed, 0 unresolved, 0 no adjacency
       0 no route, 10 unicast RPF, 0 forced drop
```

Preguntas…

Complete Your Online Session Evaluation!

Cisco.com

Por favor, complete el formulario de evaluación.

Muchas gracias.

Session AGG-2023

PPOX/L2TP Broadband Aggregation Design and Architectures