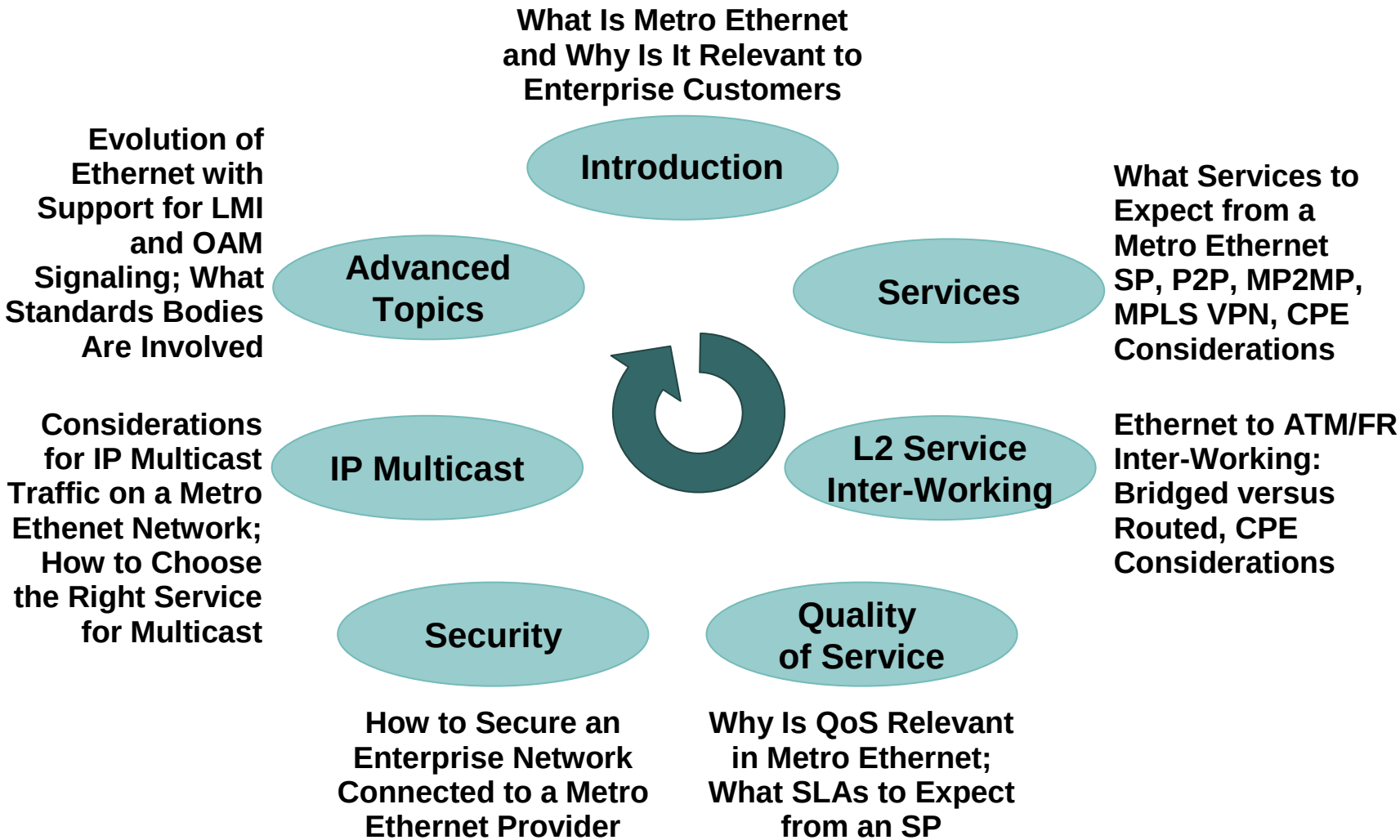
Deploying Metro Ethernet: Architecture and Services

Joe Deveaux

jdeveaux@cisco.com

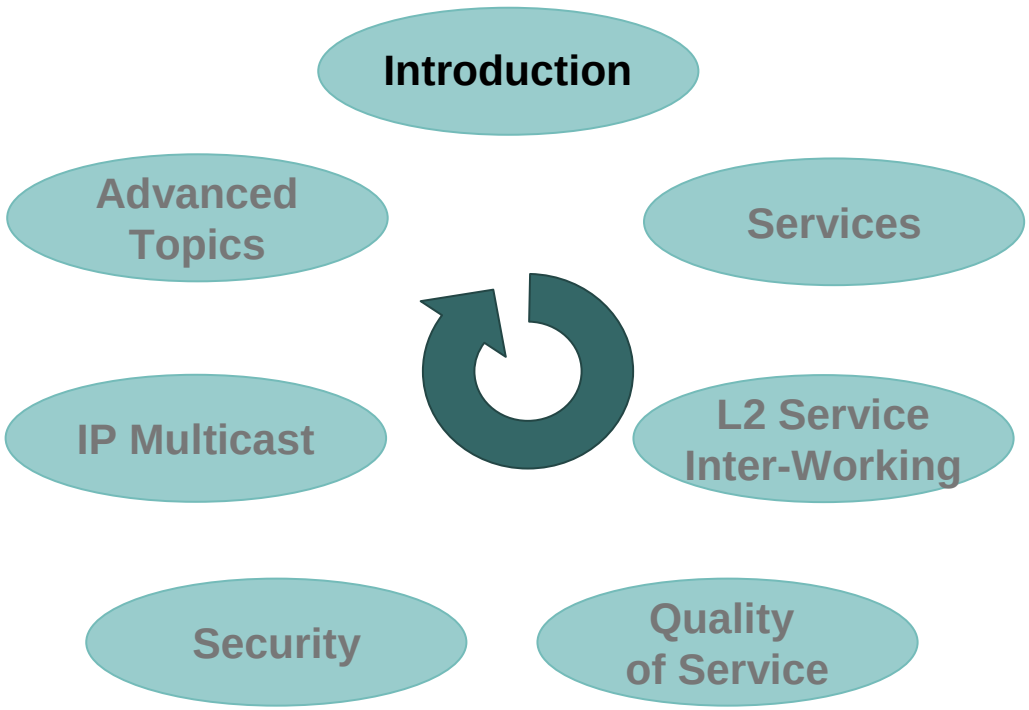
Sept 23, 2003

Agenda

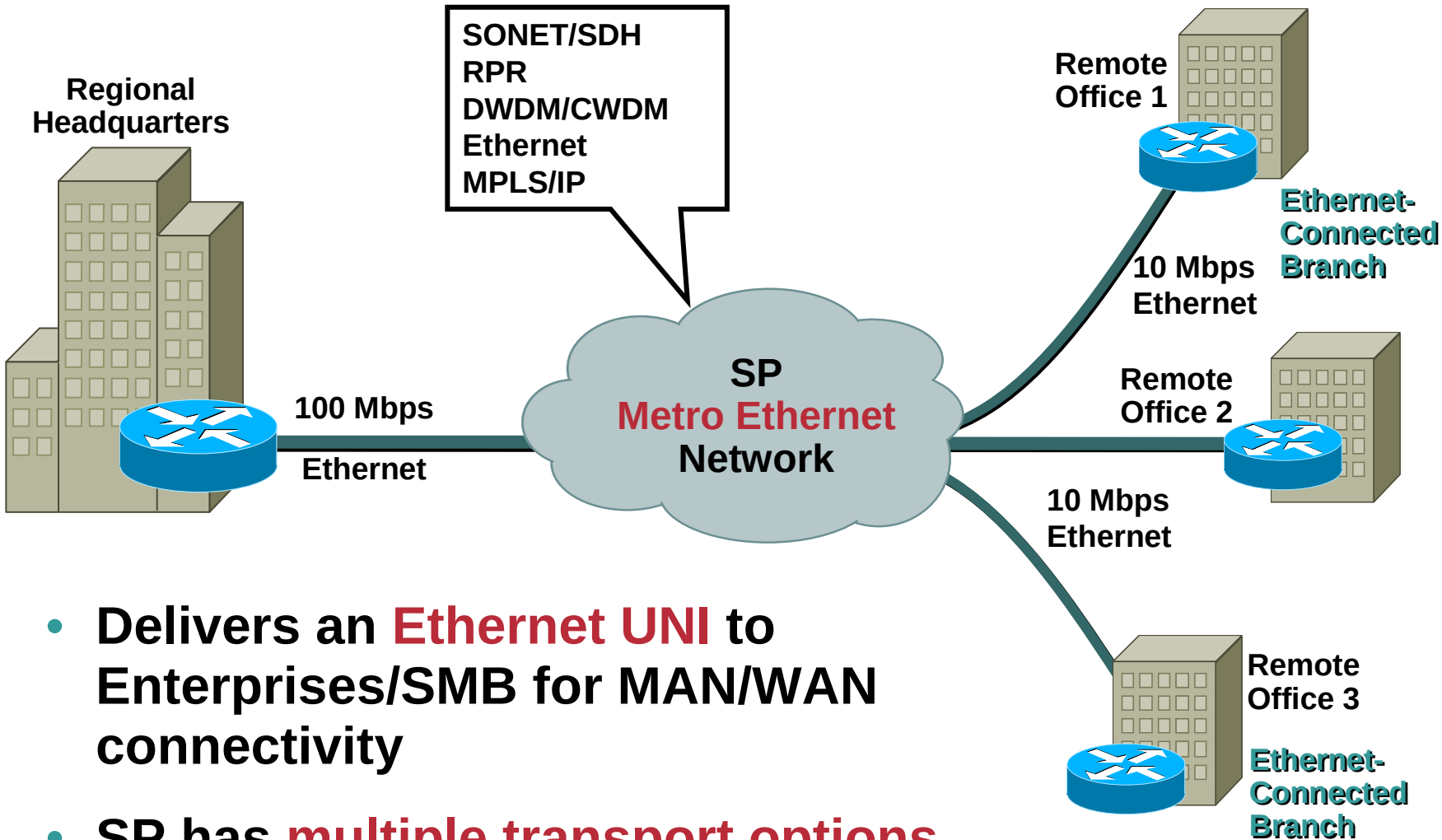


Agenda

What Is Metro Ethernet and Why Is It Relevant to Enterprise Customers



What is Metro Ethernet?



- Delivers an Ethernet UNI to Enterprises/SMB for MAN/WAN connectivity
- SP has multiple transport options

What Does Ethernet as a LAN/MAN/WAN Transport Offer?

- Ethernet becomes the ubiquitous interface: single technology for LAN, MAN and WAN
- Efficient packet-based infrastructure: IP friendly
- Cost effective interface with flexible bandwidth offerings: 10/100/1000/10000 Mbps
- Geographical independence: Ethernet over Optical, IP or MPLS

Metro Ethernet: Revolution or Evolution?

- **Questions:**

  How does Metro Ethernet change the way enterprises design and deploy networks?

  What enterprise requirements are addressed by Metro Ethernet?

- **Answers:**

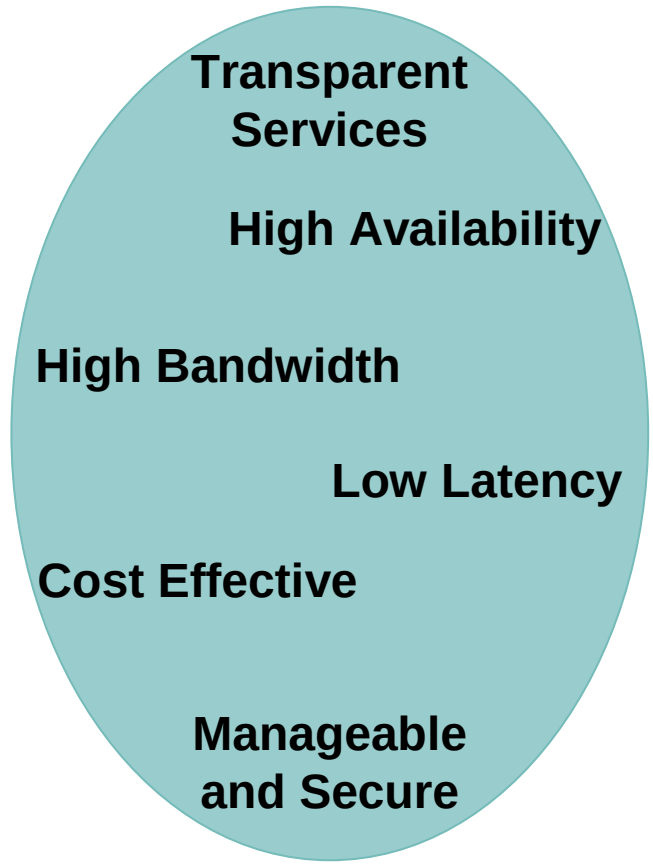
  Nothing should change; the same principles of structure and hierarchy still hold true

  Enterprise applications drive BW requirements

  Service type will dictate design considerations

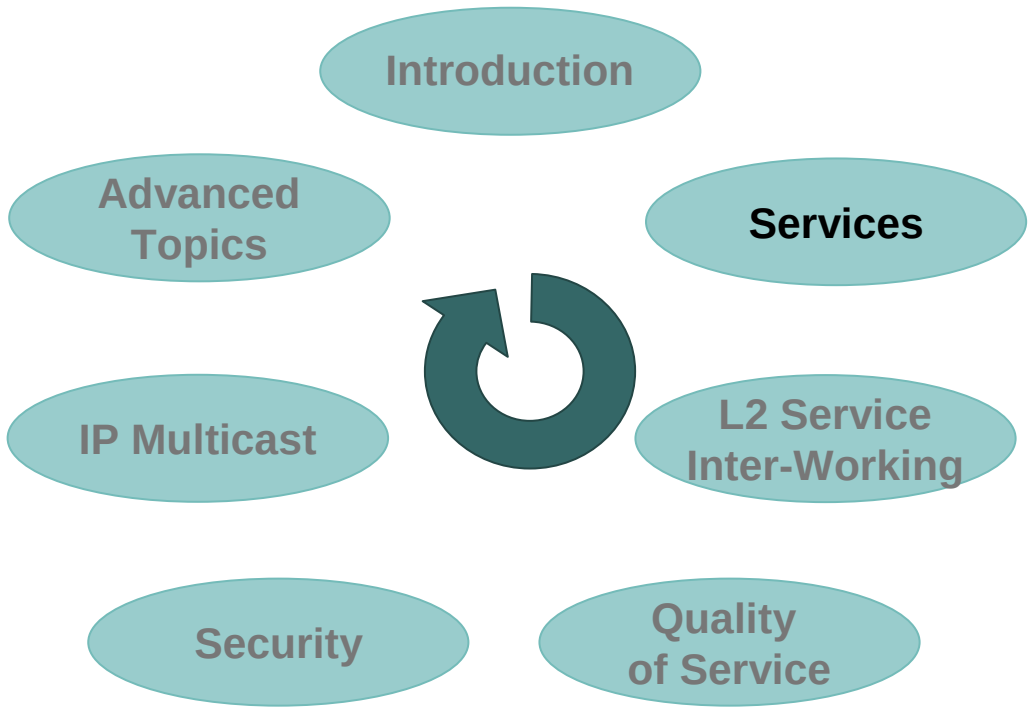
Enterprise Applications Drive Metro Ethernet

- LAN interconnect
- Service aggregation
- Interconnect data centers
- Backup and disaster recovery
- Connect to hosting services
- Value-added services



How SPs Deliver This Is Largely Irrelevant…
Metro Ethernet Is Simply a Tool in the Tool Box

Agenda

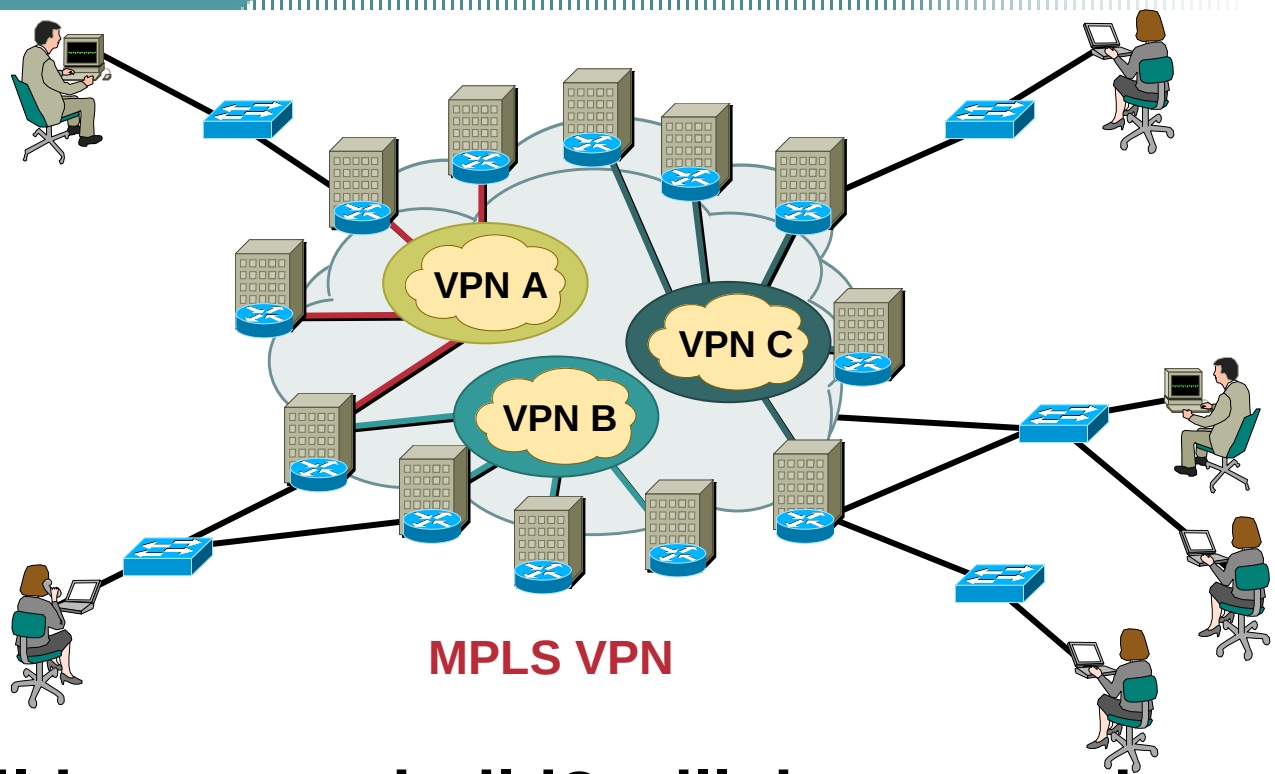


What Services to Expect from a Metro Ethernet SP, P2P, MP2MP, MPLS VPN, CPE Considerations

Metro Ethernet and L2 VPN

- FR and ATM are very common L2 VPNs
- CE has ‘n’ circuits, each connecting to other CE, in partial mesh
- Provider devices forward customer packets based on Layer 2 information (FR DLCI, ATM VC)
- Metro Ethernet is another L2 VPN where SP transports Ethernet Frames (MAC addresses could be used for forwarding decisions)
- Let’s compare now L3 VPN and L2 VPN

L2VPN versus L3VPN

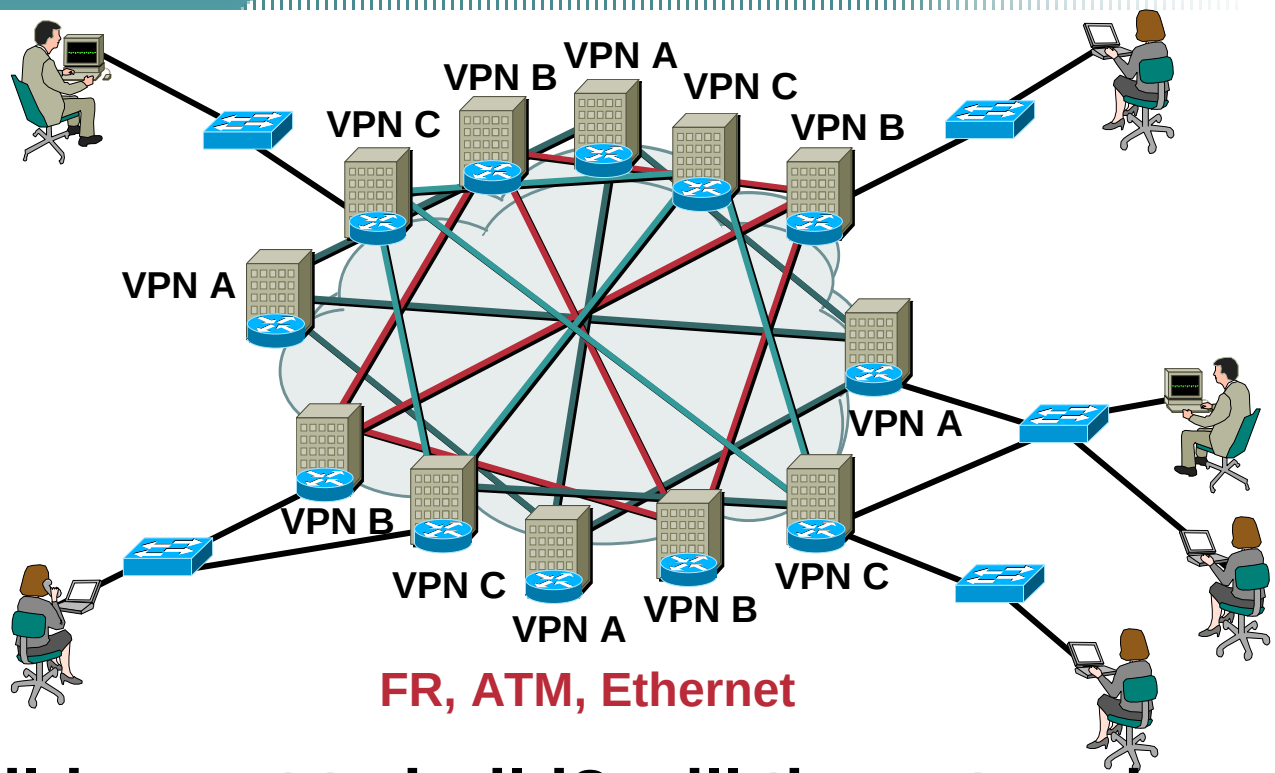


MPLS VPN

- **To build or not to build? will the enterprise…**

  Buy an SP managed IP-VPN service or

L2VPN versus L3VPN



- **To build or not to build? will the enterprise…**

  Buy an SP managed IP-VPN service or

  Buy SP's transport services in order to build their own IP network

Layer 3 and Layer 2 VPN Characteristics

Layer 3 VPNs

- SP devices forward customer packets based on Layer 3 information (e.g. IP addresses)
- SP is involved in customer IP routing
- Support for any access or backbone technology
- IP specific
- Example: RFC 2547bis VPNs (L3 MPLS-VPN)

Layer 2 VPNs

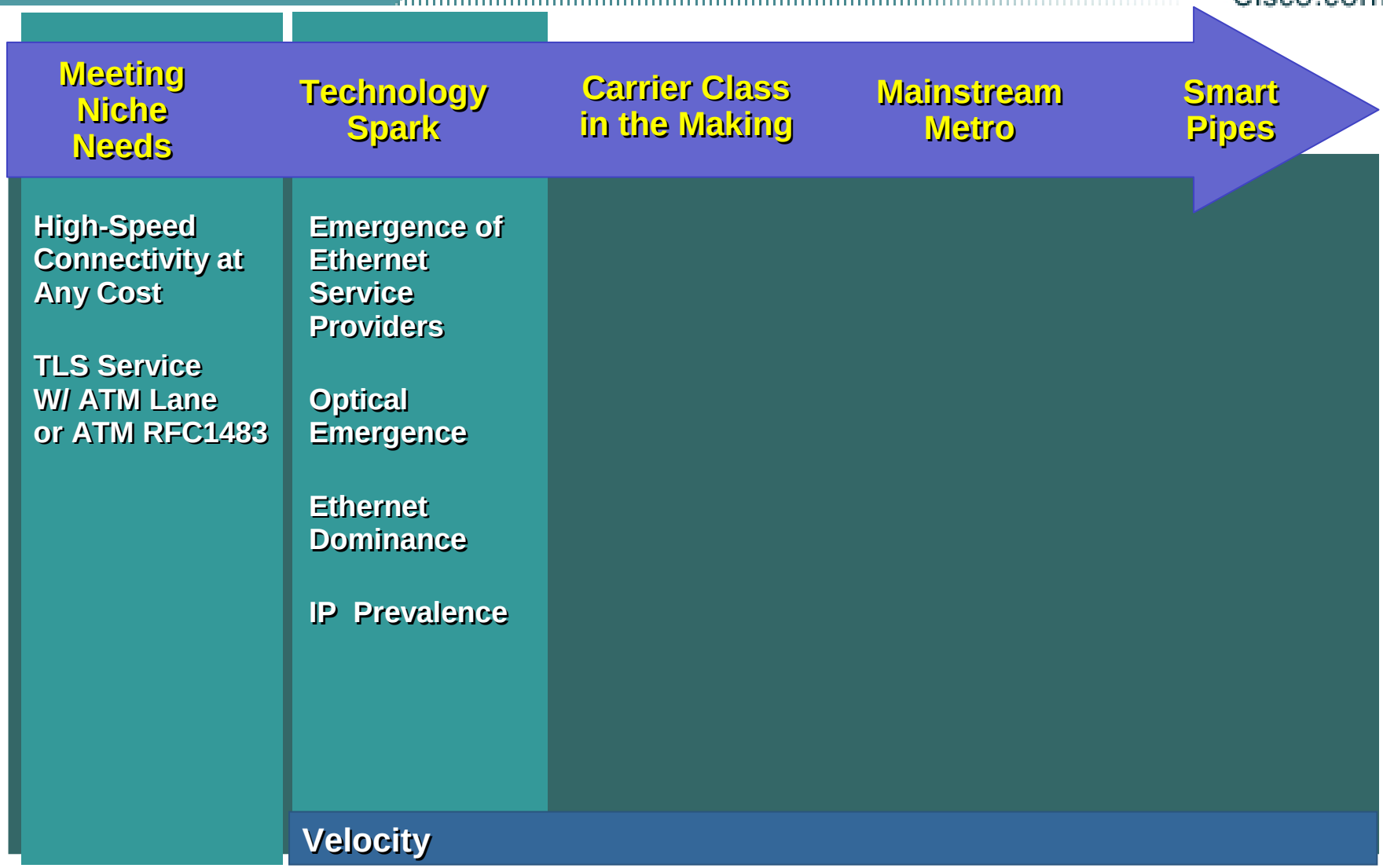
- SP devices forward customer frames based on Layer 2 information (e.g. DLCI, VPI/VCI, MAC)
- Enterprise stays in control of L3 policies (Routing, QoS)
- Access technology is determined by the VPN type
- Multiprotocol support
- Example: FR—ATM—Ethernet

Layer 3 and Layer 2 VPN Summary

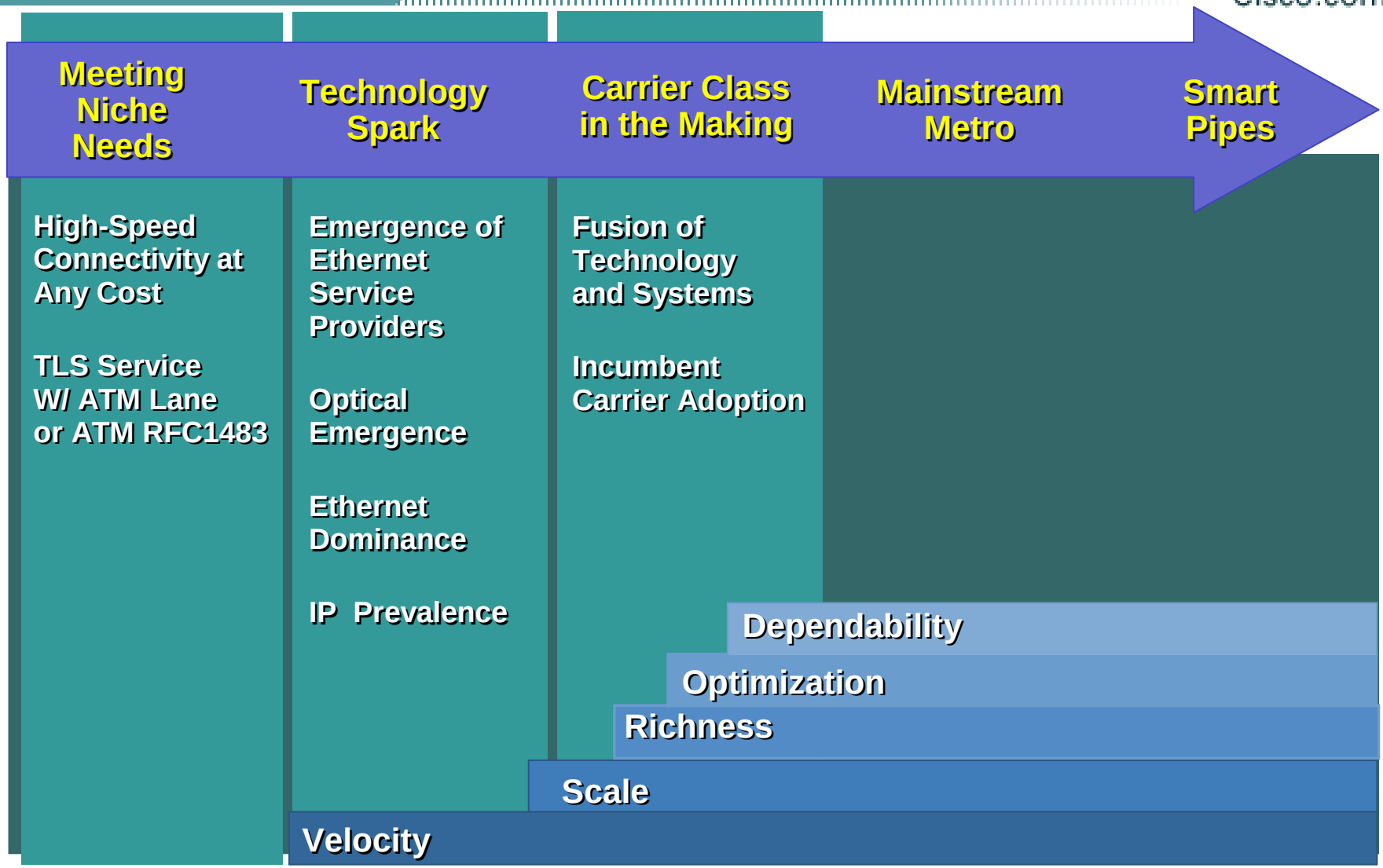
- The choice of L2VPN over L3VPN will depend on how much control the enterprise wants to retain
- Ethernet is the next natural evolution of customer UNI connection for both L2VPN or L3VPN
- L2 VPN services are complementary to L3 VPN services

  An Ethernet-based L2VPN service can be used to access L3VPNs

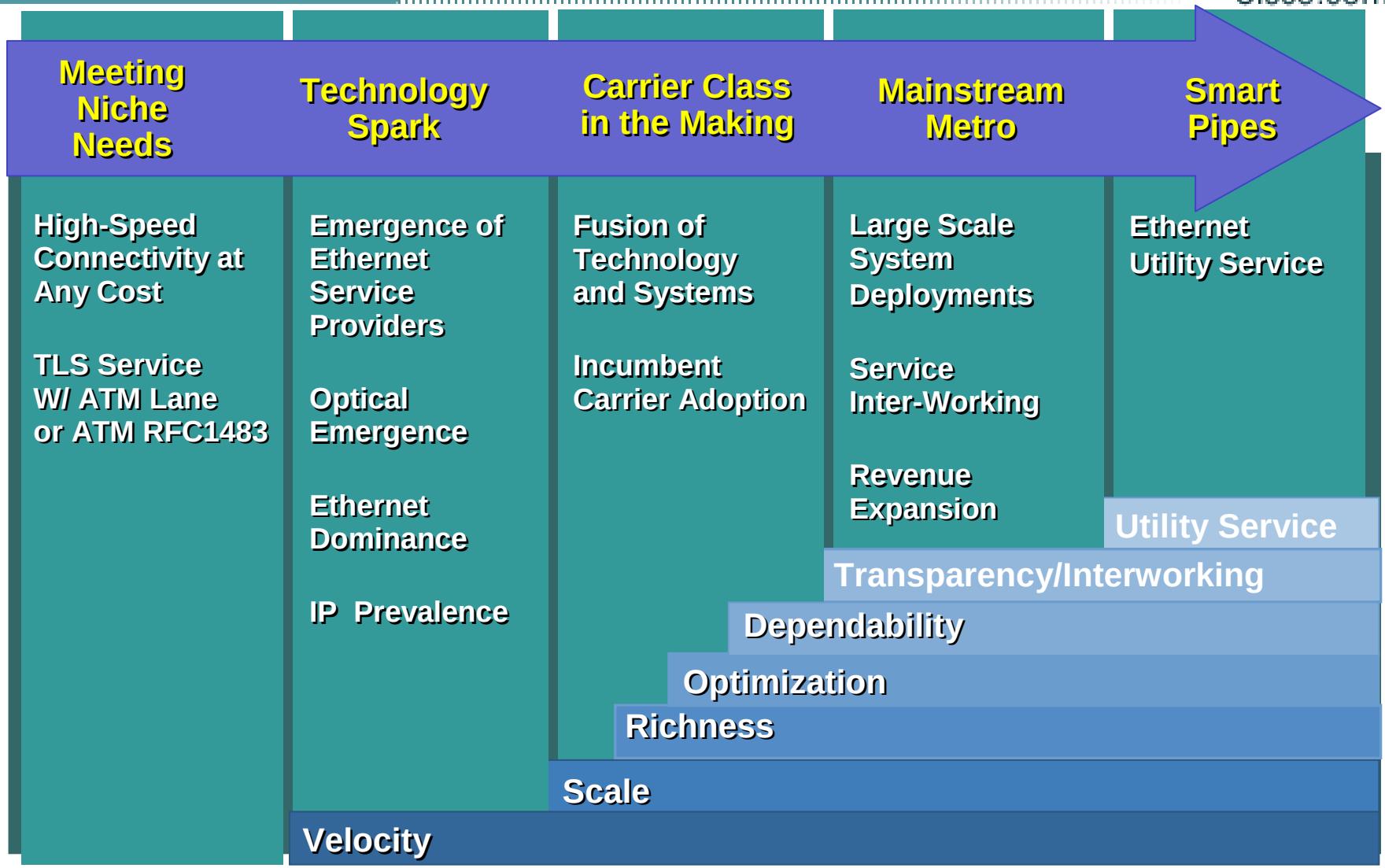
Metro Ethernet Services Evolution



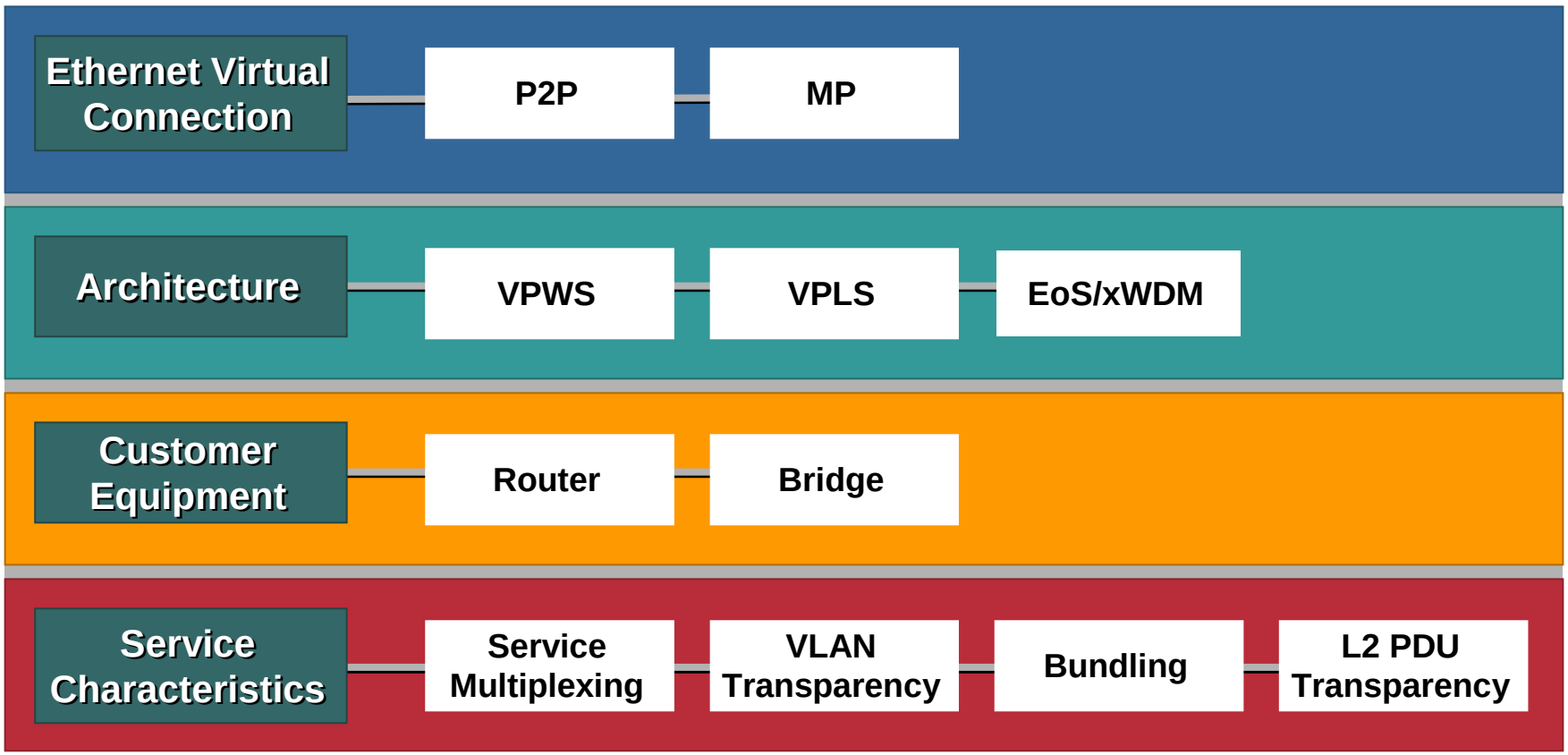
Metro Ethernet Services Evolution



Metro Ethernet Services Evolution



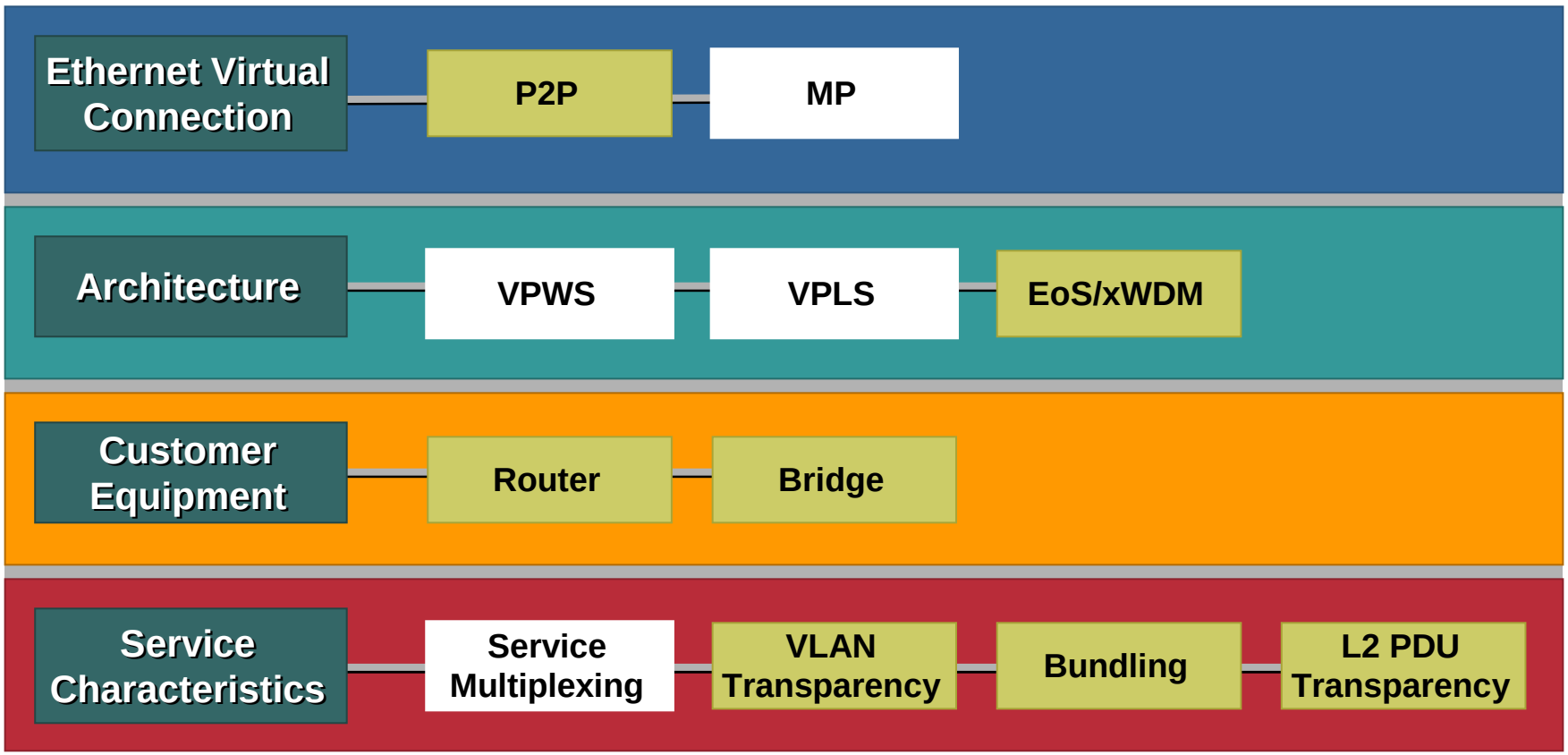
Ethernet Services
Definition Framework



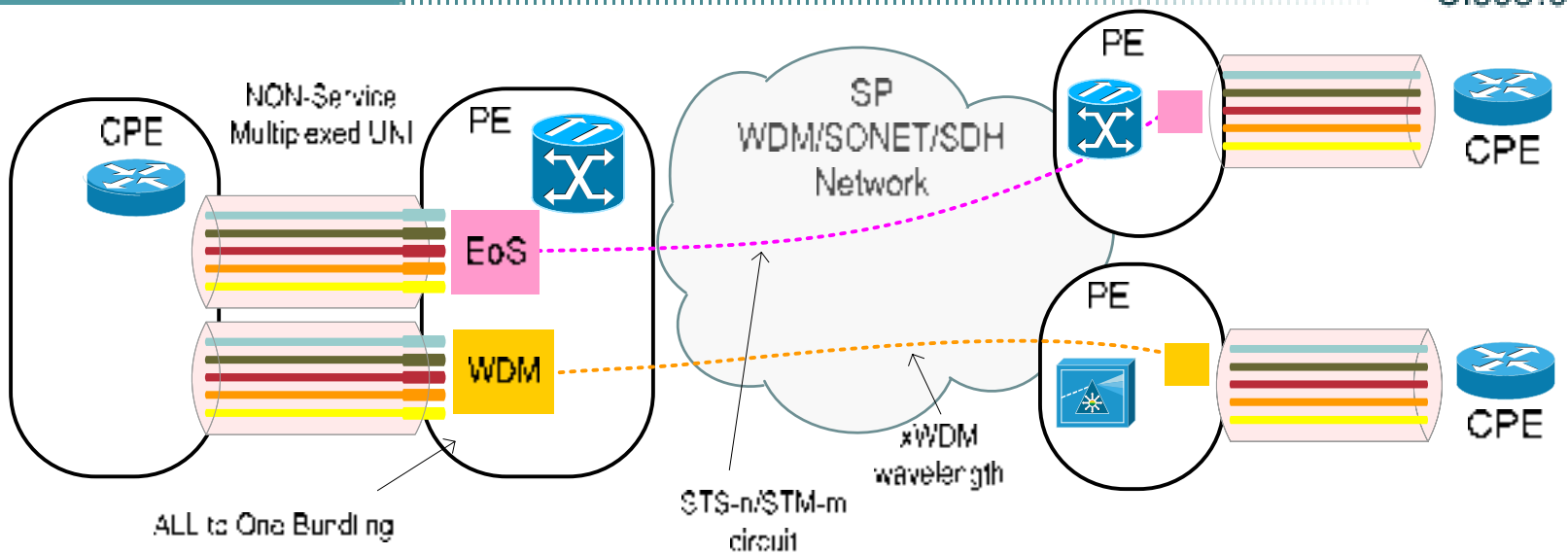
VPWS – Virtual Private Wire Service
VPLS – Virtual Private LAN Service
EoS – Ethernet over SONET/SDH

Ethernet Private Line (EPL)

Point-to-Point Port-Based Service (over SONET/SDH/xWDM)



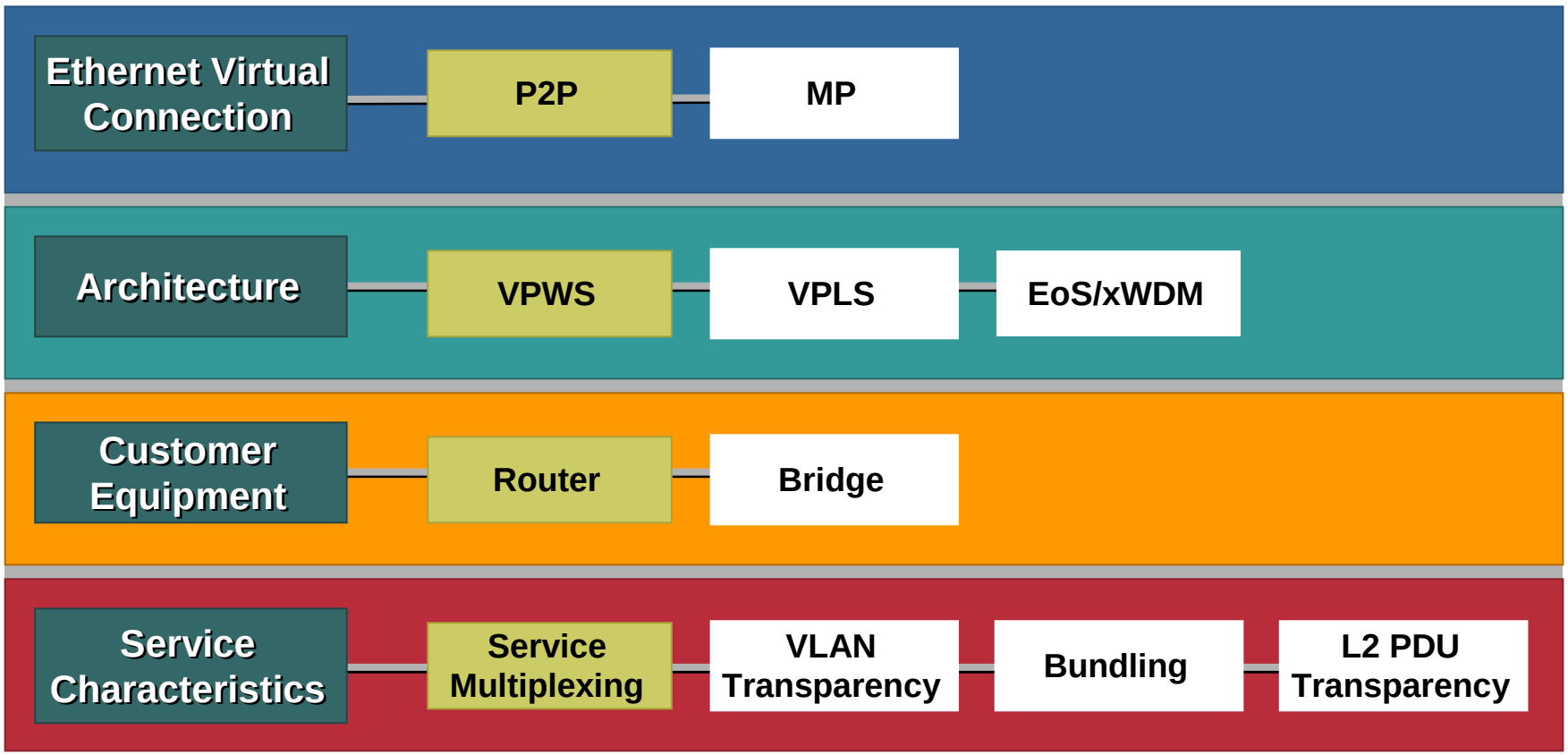
Ethernet Private Line (EPL)



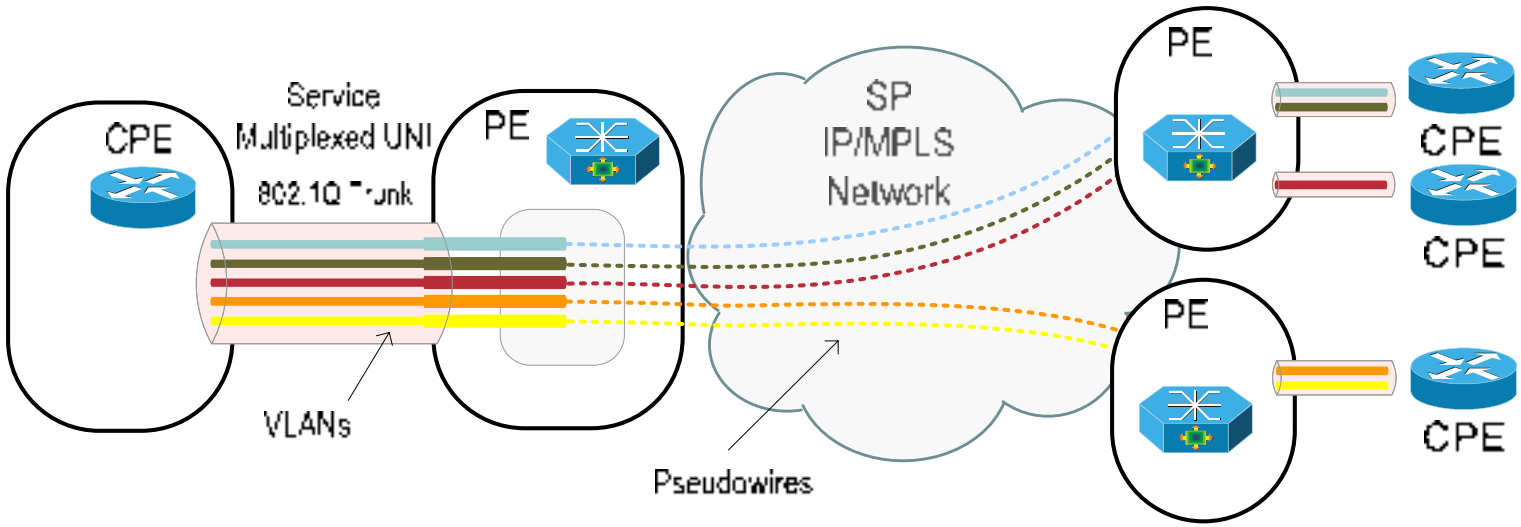
- Defines a point-to-point, port-based service
- No service multiplexing—"all-to-one" bundling
- Transparent to customer BPDUs
- Routers and switches can safely connect

Ethernet Relay Service (ERS)

Point-to-Point VLAN-Based Service



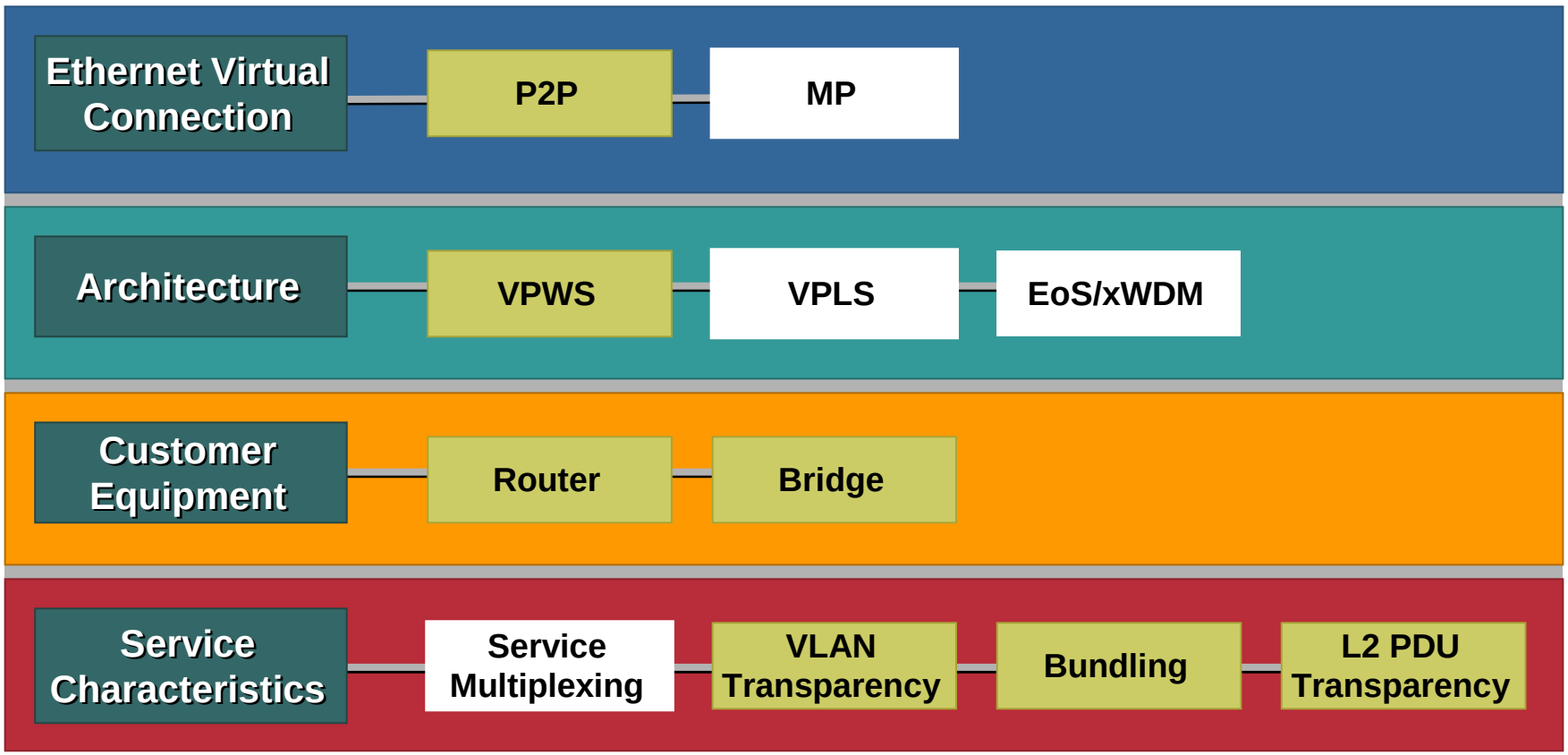
Ethernet Relay Service (ERS)



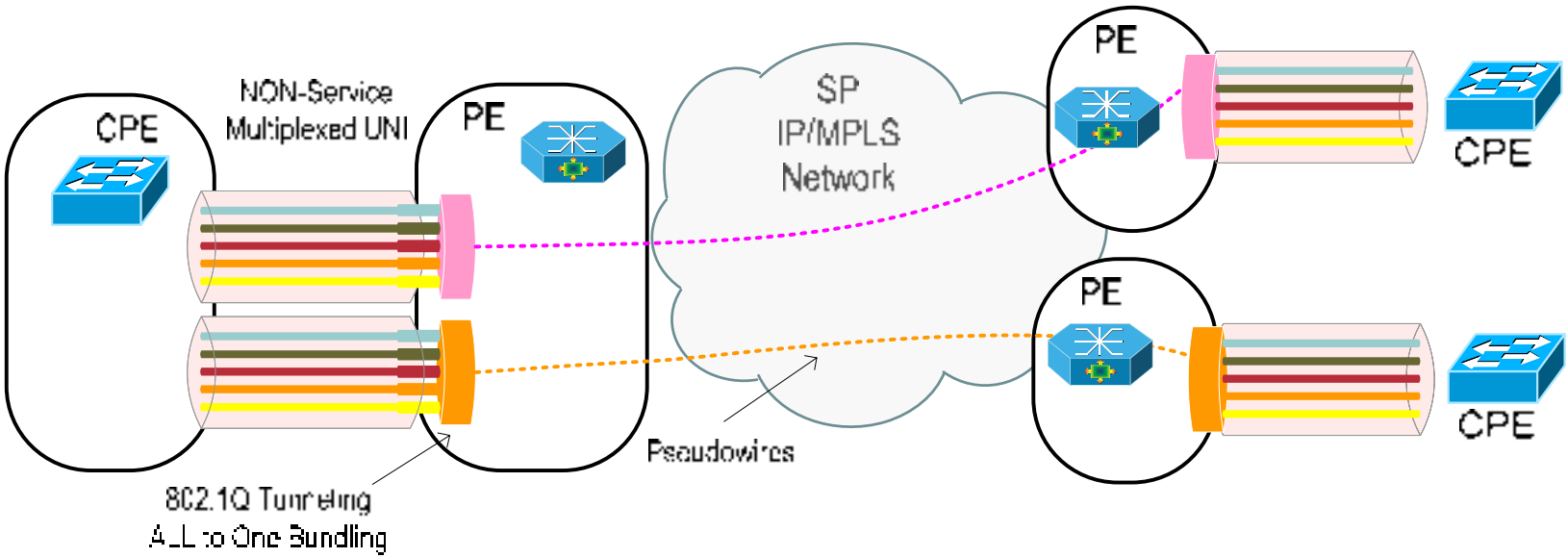
- Defines a VLAN-based point-to-point service (analogous to Frame Relay using VLAN tags as VC IDs)
- Service multiplexed UNI (e.g. 802.1Q trunk)
- Opaque to customer PDUs (e.g. BPDUs)
- Encourage a router as CPE edge device

Ethernet Wire Service (EWS)

Point-to-Point Port-Based Service



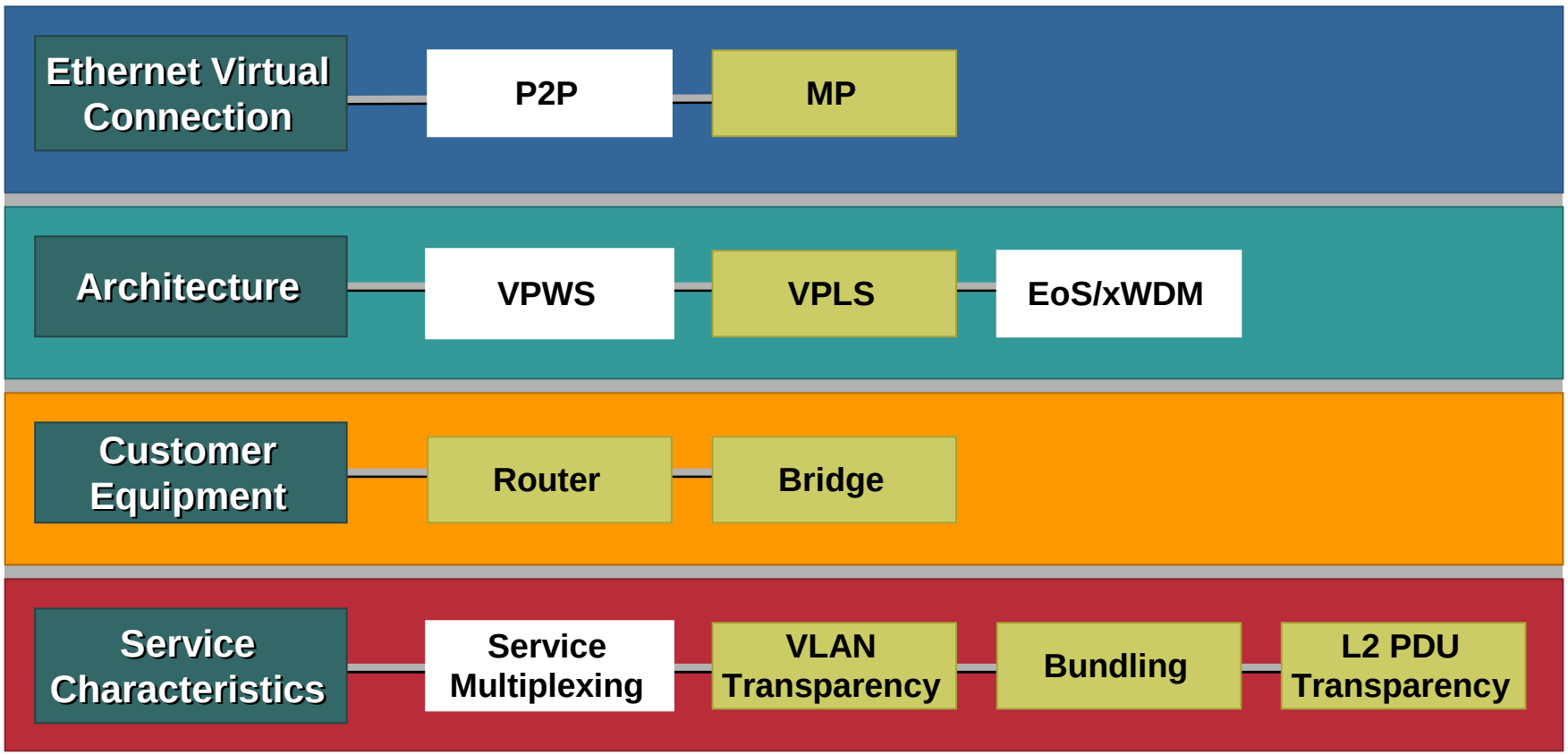
Ethernet Wire Service (EWS)



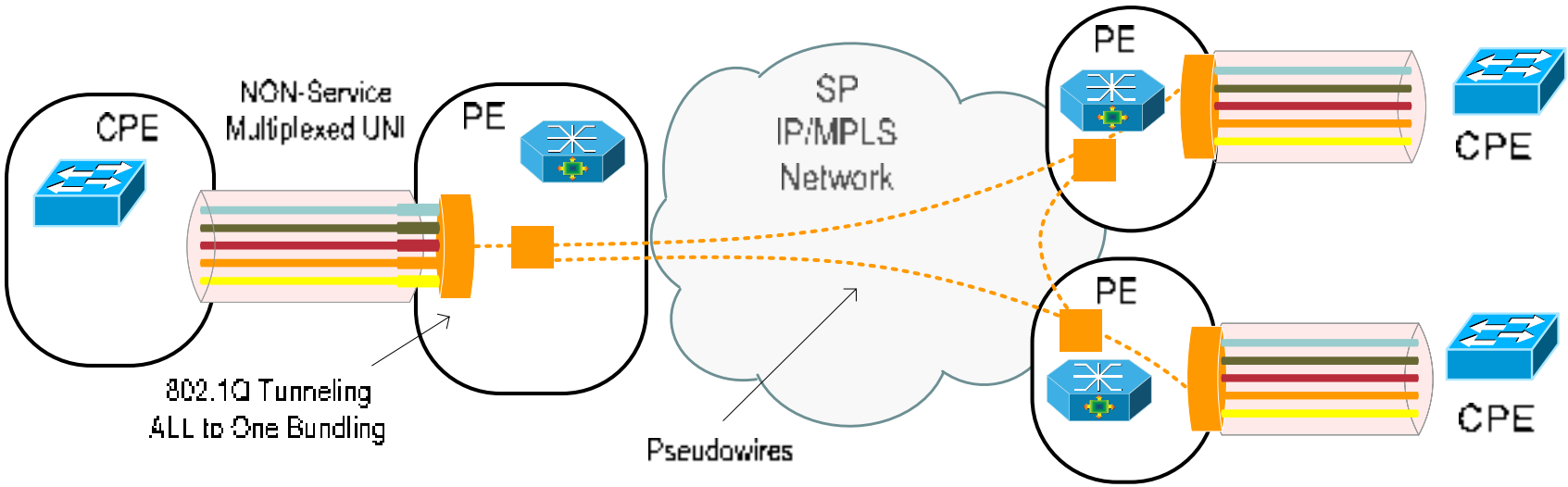
- Defines a point-to-point, port-based service
- No service multiplexing—"all-to-one" bundling
- Transparent to customer BPDUs
- Routers and switches can safely connect

Ethernet Multipoint Service (EMS)

Multipoint Port-Based Service



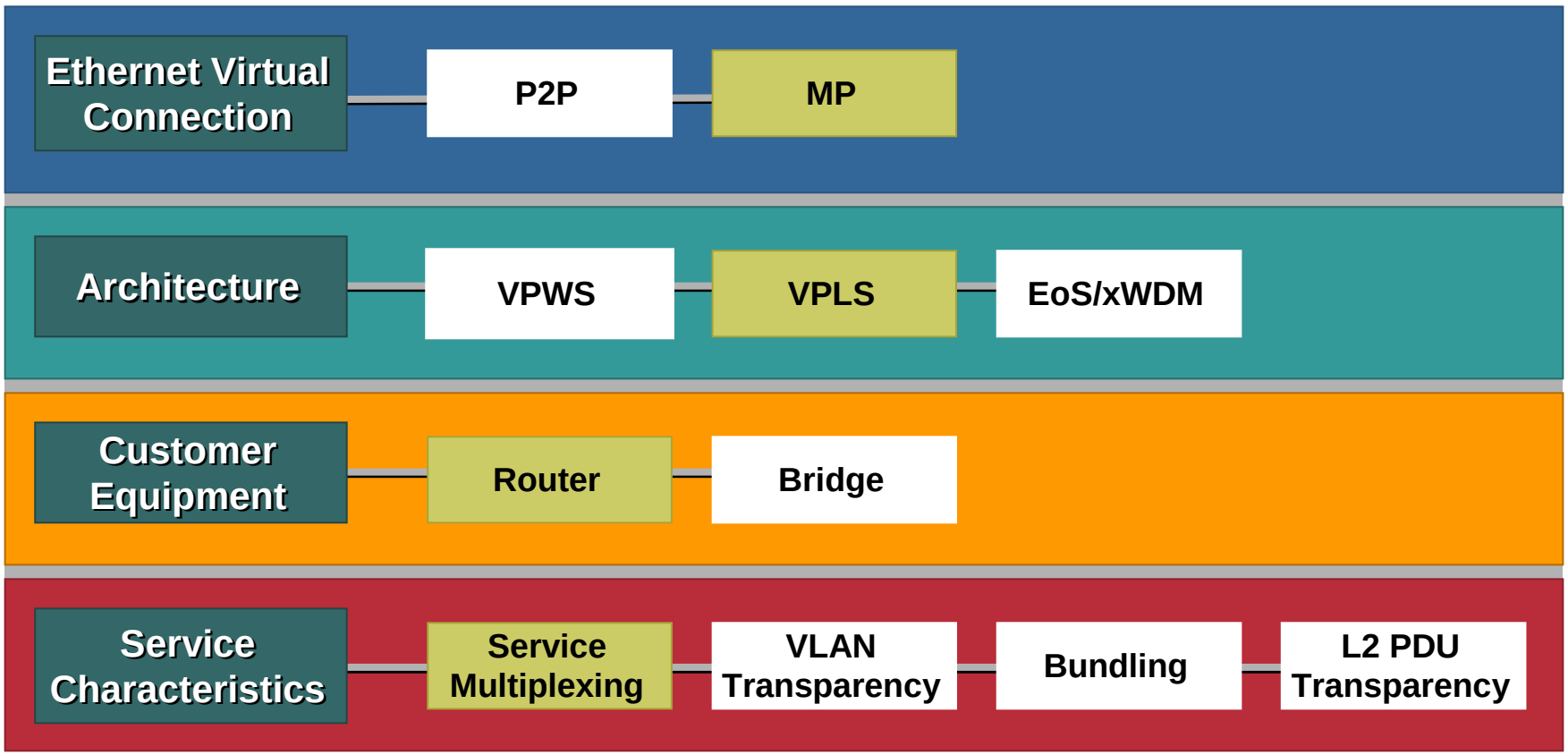
Ethernet Multipoint Service (EMS)



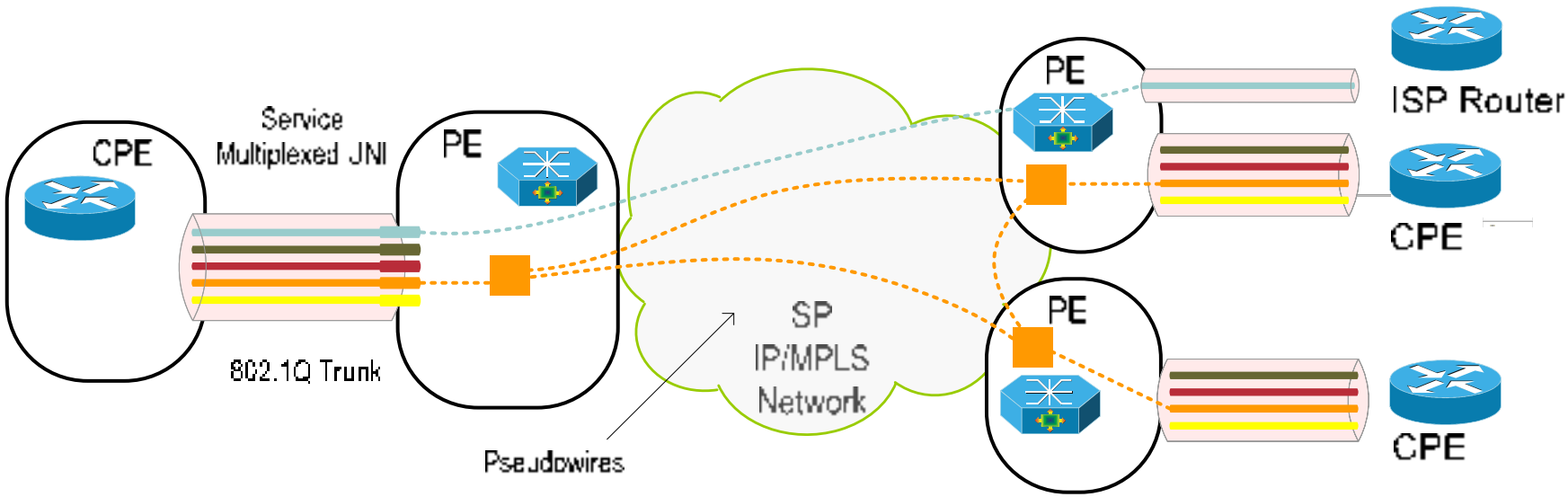
- **Multipoint service where all devices are direct peers**
- **No service multiplexing—all VLANs are presented to all sites (“all-to-one” bundling)**
- **Transparent to customer BPDUs**
- **AKA Transparent LAN Service (TLS) or E-LAN**
- **Routers and switches can safely connect**

Ethernet Relay Multipoint Service (ERMS)

Multipoint VLAN-Based Service

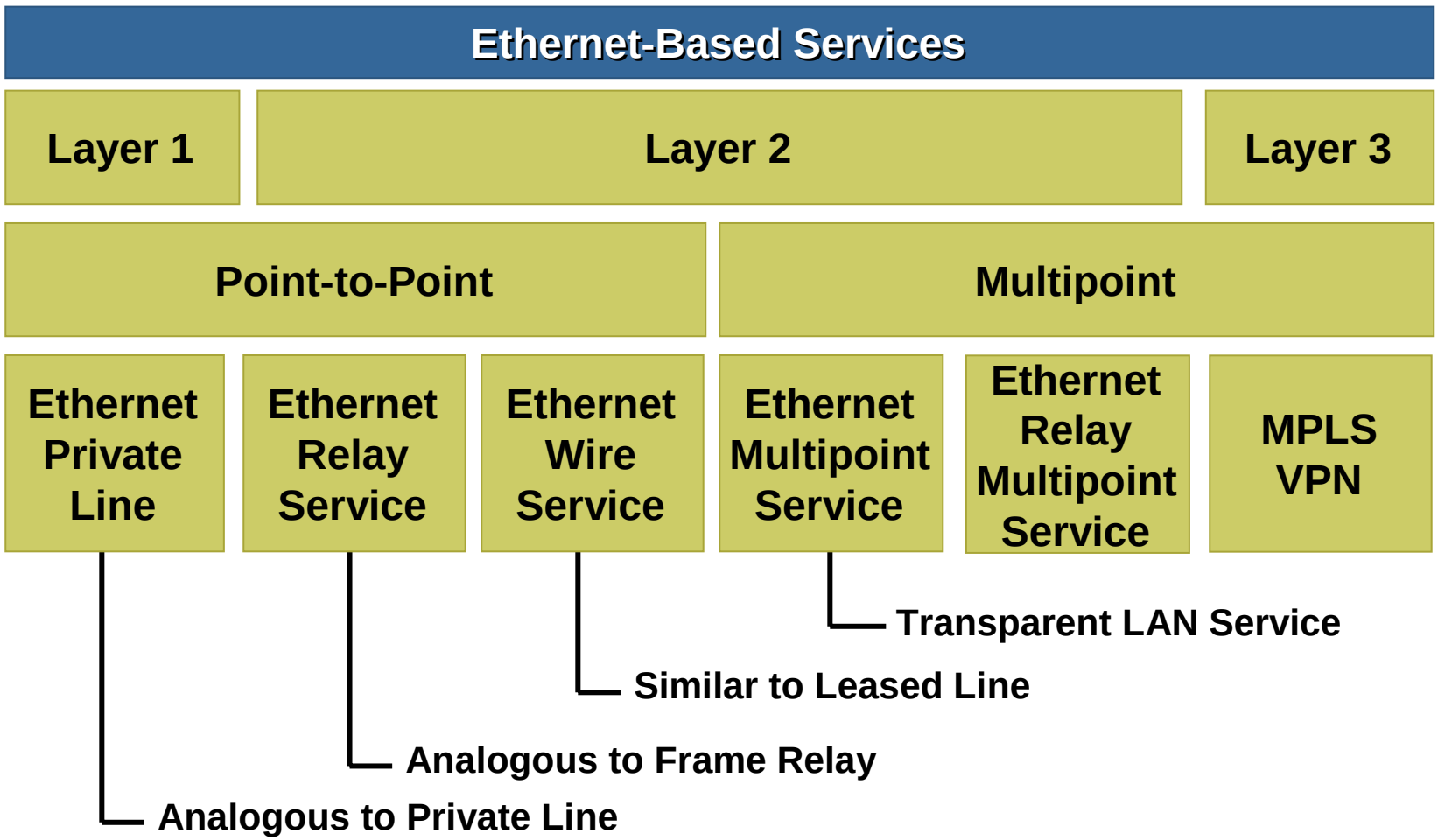


Ethernet Relay Multipoint Service (ERMS)



- **Both P2P and MP2MP Services can coexist on the same UNI**
- **Service multiplexed UNI (e.g. 802.1Q trunk)**
- **Opaque to customer PDUs (e.g. BPDUs)**
- **Routers can safely connect to an ERMS UNI**

Summary of Ethernet-Based Services



Summary of Service Attributes for Ethernet-Based Services

	Ethernet Relay Service**	Ethernet Relay Multipoint Service**	Ethernet Wire Service**	Ethernet Private Line**	Ethernet Multipoint Service**
EVC Type	Point-to-Point	Multipoint and Point-to-Point	Point-to-Point	Point-to-Point	Multipoint
Service Multiplexed UNI	Yes	Yes	No	No	No
CE-VLAN Transparency	No	No	Yes	Yes	Yes
Bundling	None	None	All to One	All to One	All to One
Bandwidth Profile	Yes	Yes	Yes	Yes	Yes
Over-subscription	Yes	Yes	Yes	No	Yes
Layer 2 PDU Transparency	Discard CDP, VTP, STP*	Discard CDP, VTP, STP*	Tunnel CDP, VTP, STP*	Tunnel CDP, VTP, STP*	Tunnel CDP, VTP, STP*
CPE Type	Router***	Router***	Router or Switch	Router or Switch	Router or Switch

***Pause, LACP, and Port Authentication are Processed or Discarded at UNI**
****Cisco Terminology**
***** Switches May Attach in Certain Configurations**

Layer 2 Ethernet Services Comparison

- P2P and MP2MP compared as the Enterprise Network grows

- Point-to-Point (ERS and EWS)
  - Models ATM/Frame Relay
  - Complex configuration
  - Predictable traffic patterns
  - Simple QoS and security policy definition
  - Simple IGP peering
  - Simple IP multicast behaviour
  - Simple troubleshooting

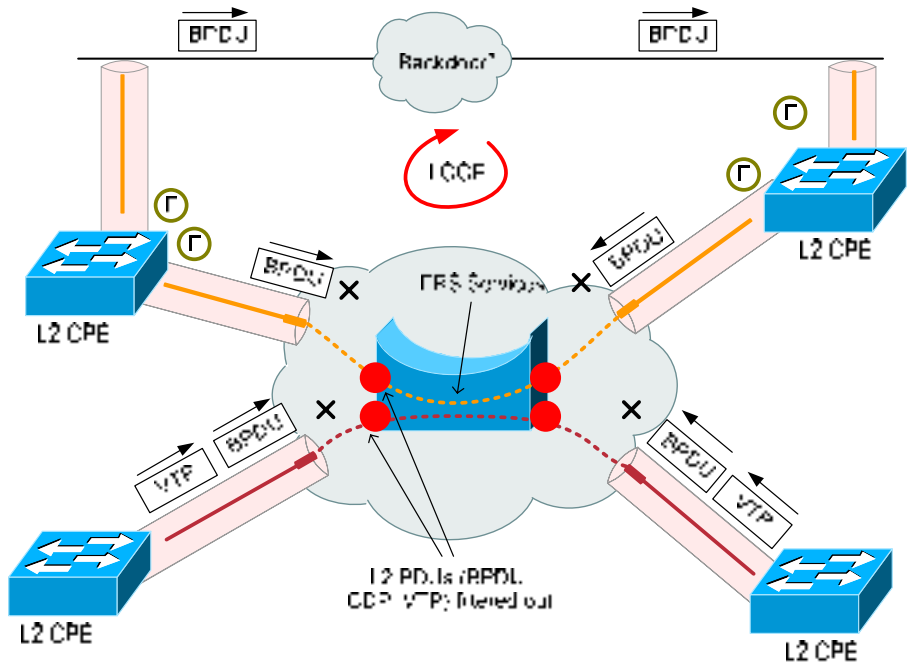
- Multipoint (EMS and ERMS)
  - New WAN broadcast model
  - Simple configuration
  - Unpredictable traffic patterns
  - Complex QoS and security policy definition
  - Complex IGP peering
  - Complex IP multicast behaviour
  - Complex troubleshooting

CPE Considerations

- **Questions:**
  - **Can I connect switches to an ERS service?**
  - **Can I connect routers to an EWS service?**
  - **Do I need to worry about the STP protocol I am running on my switches?**
  - **What are the valid CPE combinations?**
- **Lets look at some scenarios…**

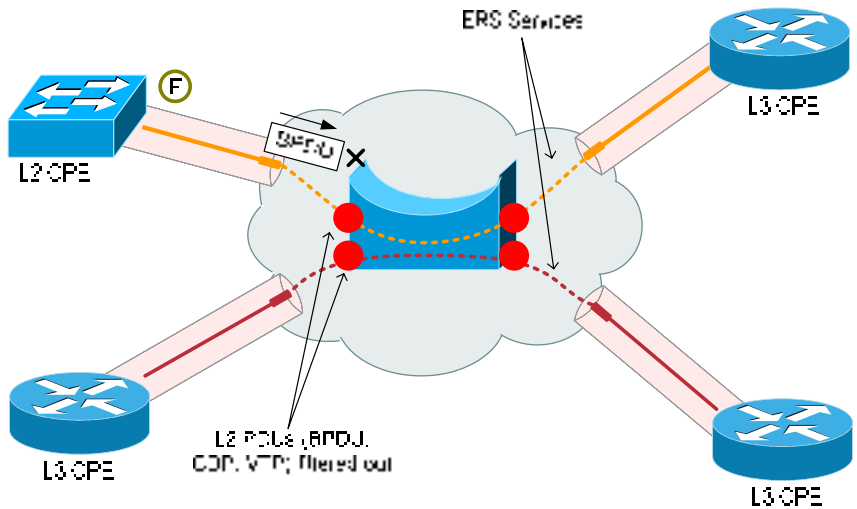
CPE Considerations—ERS and L2 Switches

- ERS is a VLAN service opaque to L2 PDUs
- L2 CPE must use VLAN IDs determined by SP
- STP loops cannot be detected in the presence of "Backdoors"
- A "Backdoor" could be a service from another SP
- In a loop-free scenario:
  - STP domain partitioned, one root on each side
  - VTP advertisements will not flow end-to-end



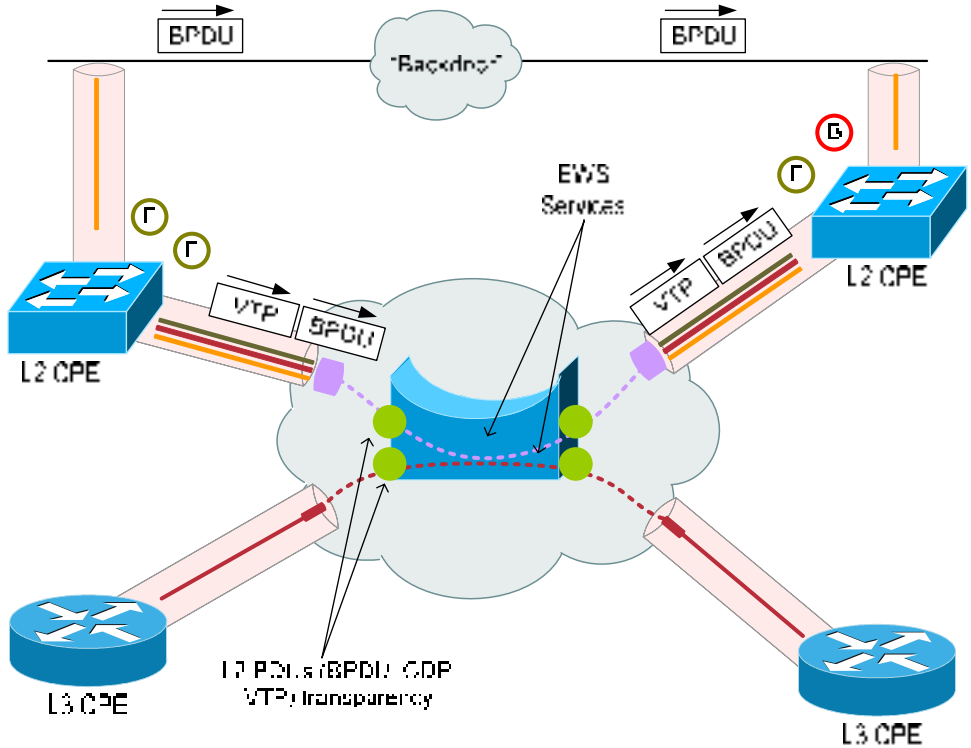
CPE Considerations— ERS Valid Combinations

- ERS is mainly intended for L3 CPEs or any other scenarios where L2 PDU transparency is not required
- SP should protect the UNI against un-expected L2 PDUs
- L2 CPE to L3 CPE is another valid combination

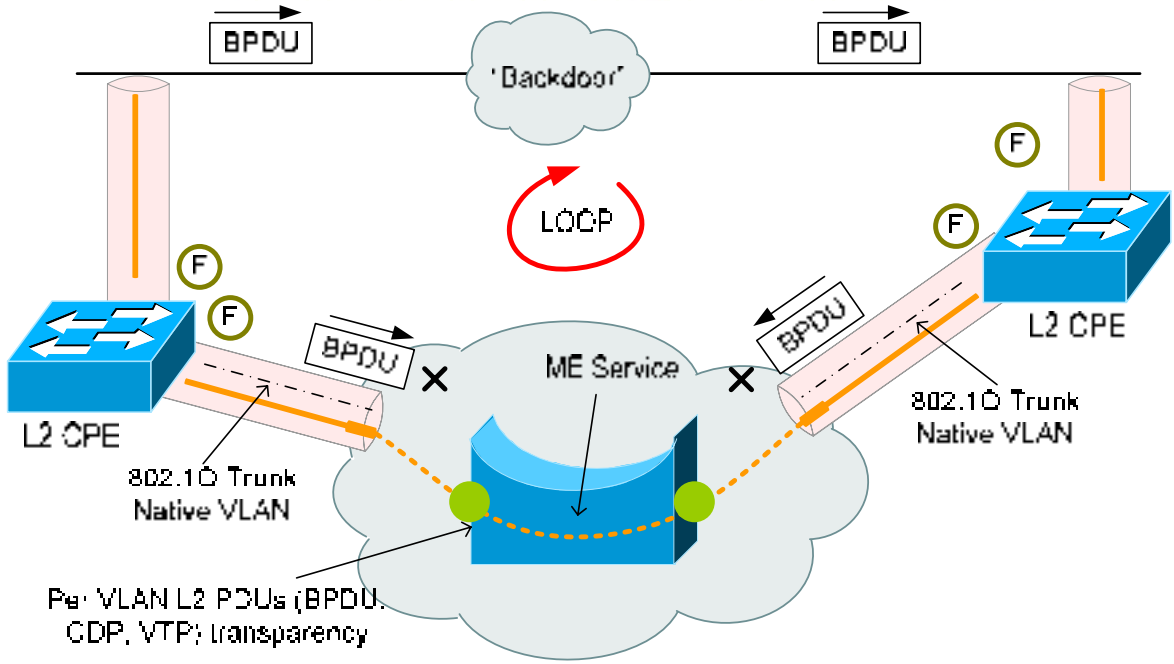


CPE Considerations— EWS Valid Combinations

- EWS is a port based service with L2 PDU transparency
- External loops can be detected by the end devices
- Both L2 and L3 CPEs can be connected to an EWS UNI

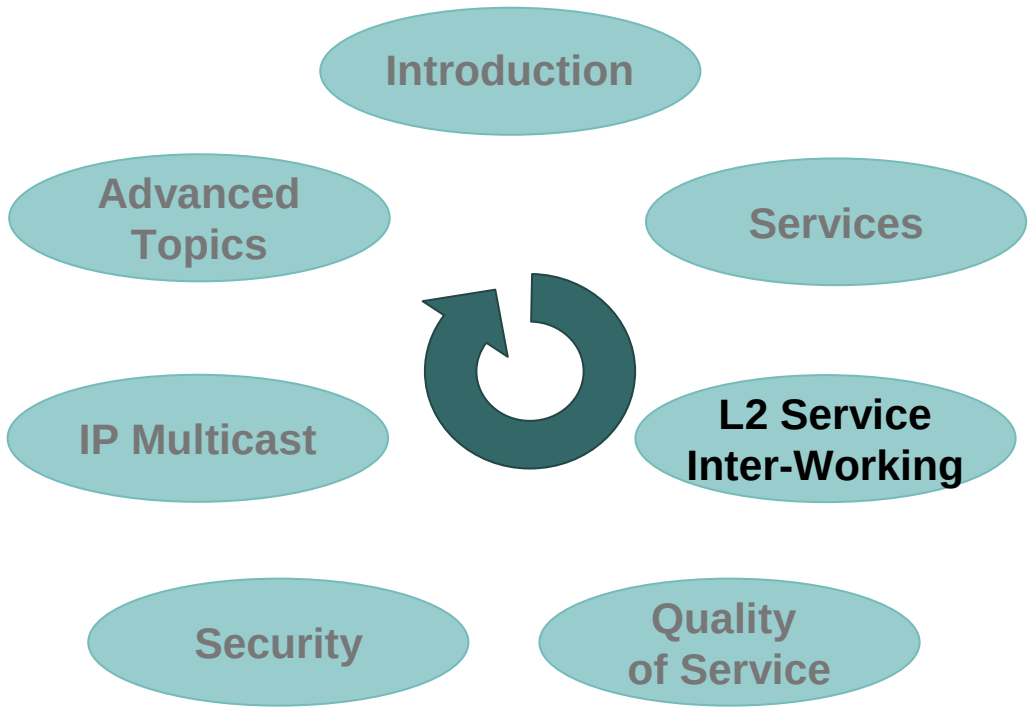


CPE Considerations—CPE STP Protocol



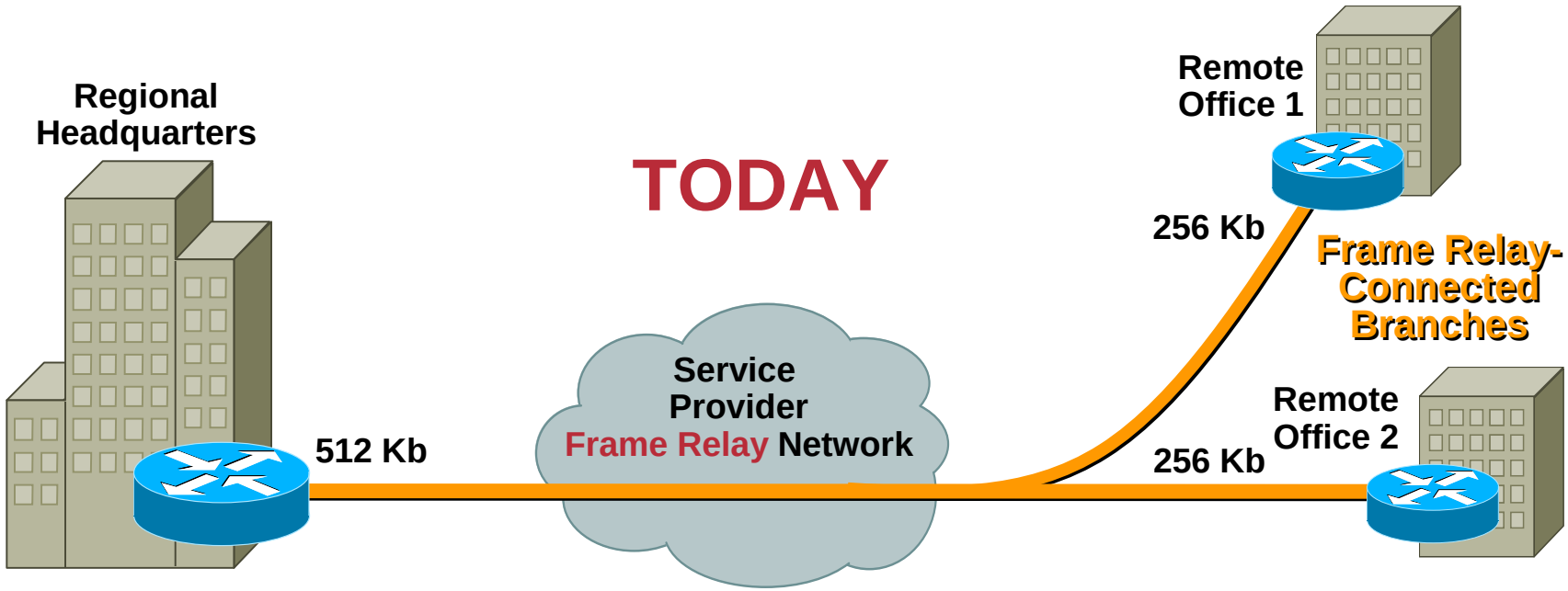
- **IEEE BPDUs (0x0180 c200 0000) are always transmitted untagged, compared to PVST+ BPDUs (always tagged)**
- **If contracting a VLAN-based service with L2 transparency, make sure that the native VLAN is carried everywhere**
- **Affects P2P or MP2MP services**

Agenda



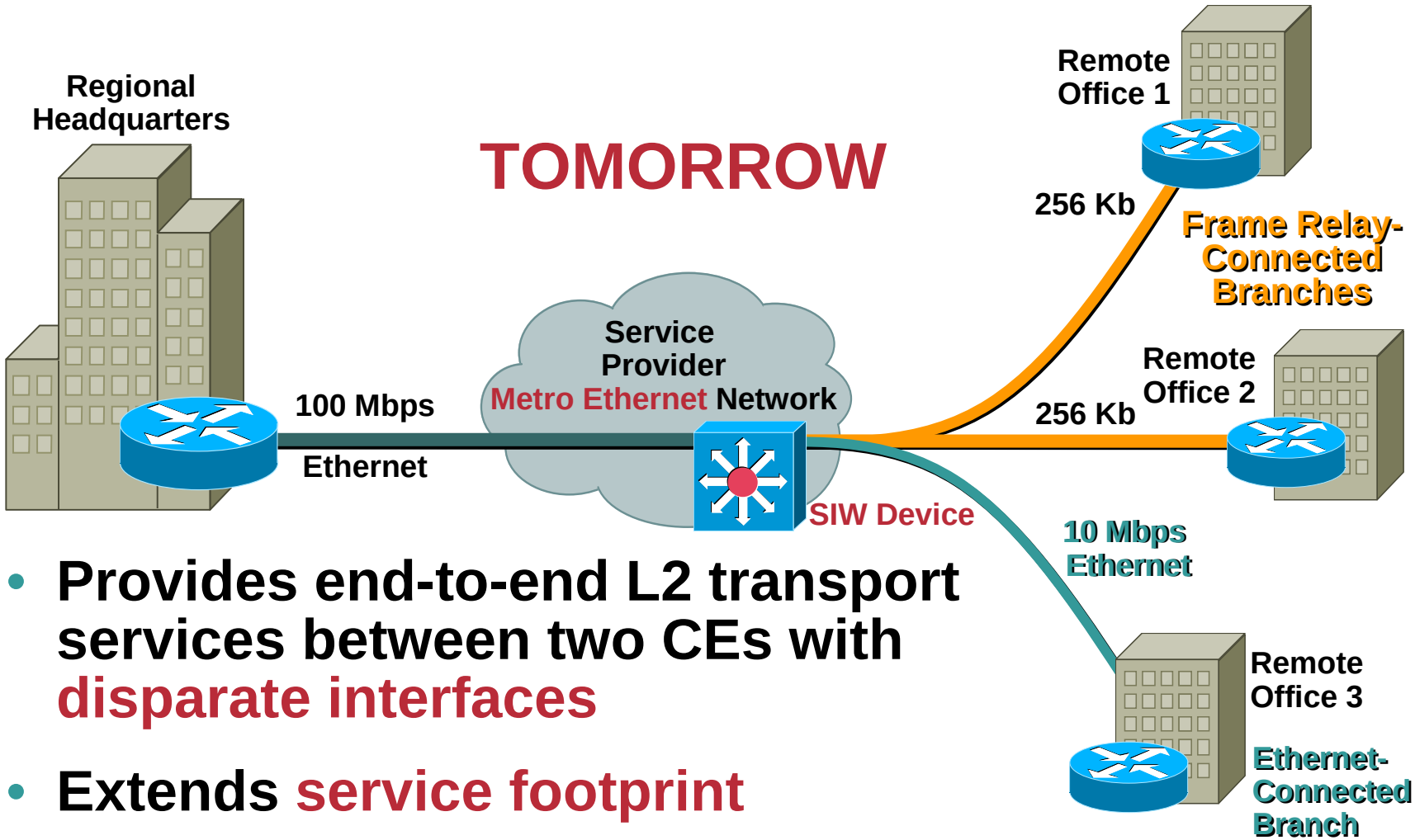
Ethernet to ATM/FR Inter-Working: Bridged versus Routed, CPE Considerations

Ethernet to Frame/ATM Inter-Working



- **Why and when is Service Inter-Working (SIW) needed in Metro Ethernet?**
- **Let's examine Layer 2 SIW in the context of Metro Ethernet…**

Ethernet to Frame/ATM Inter-Working



- **Provides end-to-end L2 transport services between two CEs with disparate interfaces**
- **Extends service footprint**

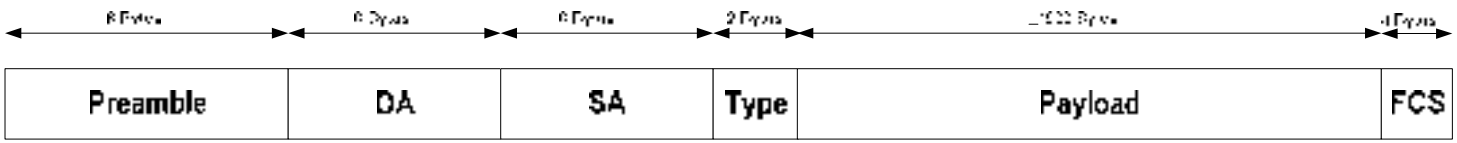
BUT It Is Not Trivial !!!

Layer 2 Service Inter-Working Complexities

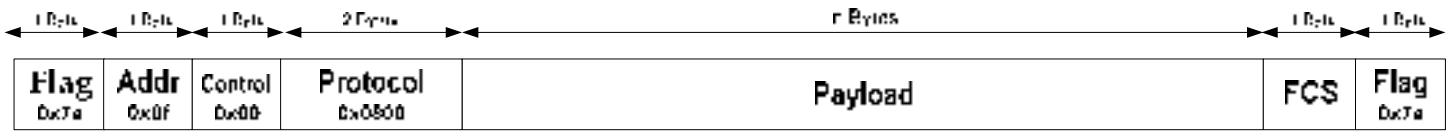
- **Each Layer 2 Protocol has different frame format**
  - **Ethernet has Layer 2 source and destination addresses**
  - **Frame Relay and ATM have a destination address only**
  - **Frame Relay and ATM have routed and bridged encapsulations**
  - **HDLC and PPP have no addresses**

Layer 2 Protocols Frame Formats

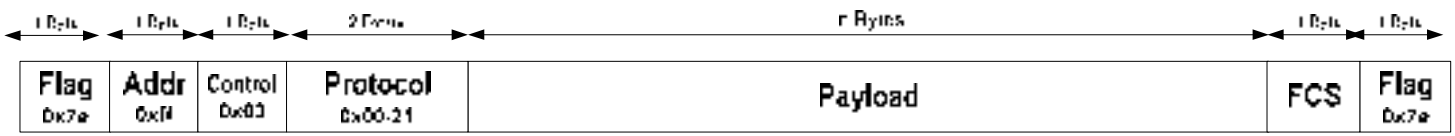
Ethernet Frame Format



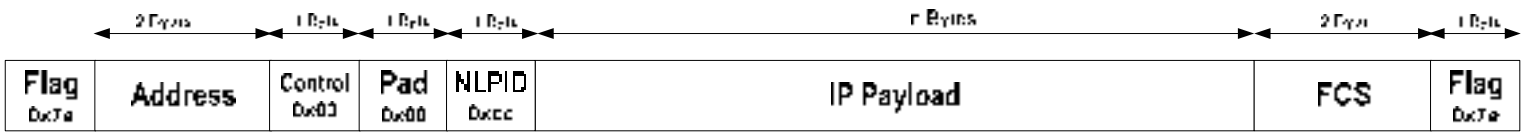
HDLC Frame Format



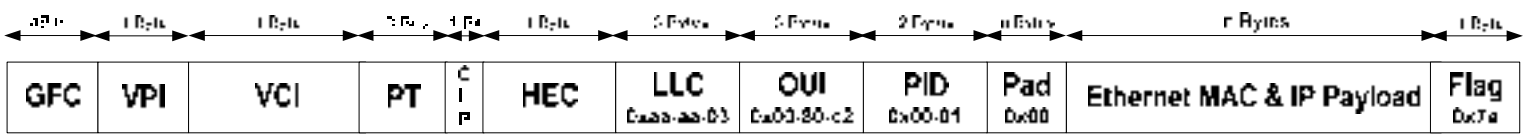
PPP Frame Format



Frame Relay Frame Format - RFC2427 Routed IP Encapsulation



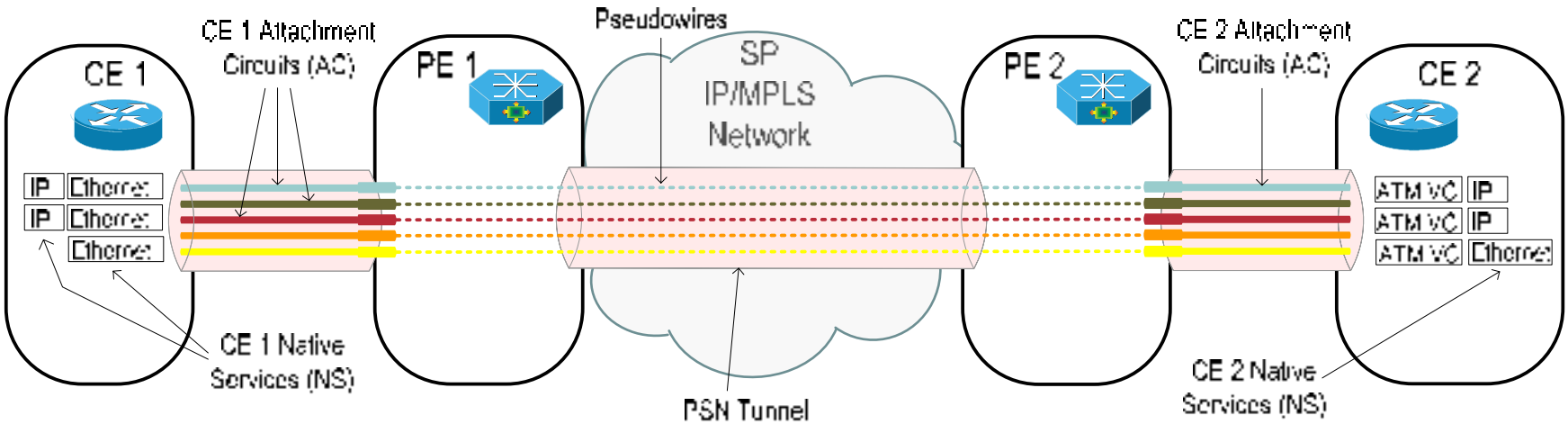
ATM Frame Format - RFC2684 Bridged IP Encapsulation



Layer 2 Service Inter-Working Complexities

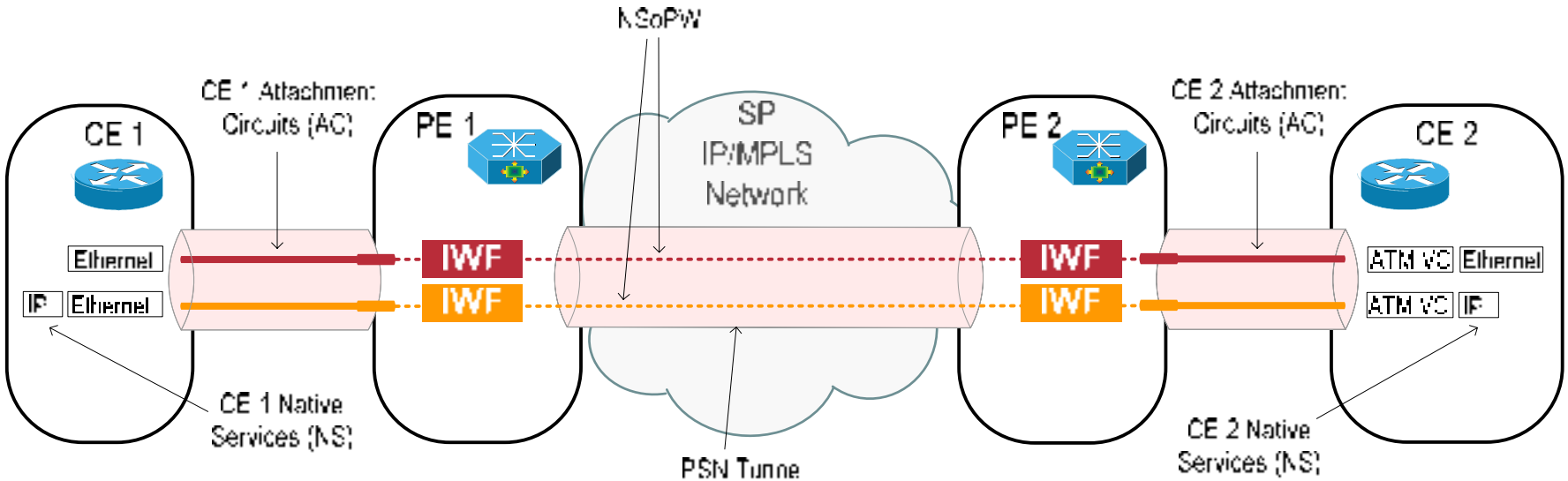
- **Each Layer 2 protocol has different address resolution processes**
  - **Ethernet uses IP ARP**
    - **The target Layer 3 address is known but not the Layer 2 address**
  - **HDLC and PPP interfaces do not ARP**
    - **It's point-to-point so they simply transmit**
    - **PPP uses NCP, but not as an ARP mechanism**
  - **ATM and Frame Relay Multipoint interfaces use Inverse ARP**
    - **The target Layer 2 address is known but not the Layer 3 address**
  - **ATM and Frame Relay p2p interfaces do not inverse ARP**
    - **It's point-to-point so they simply transmit**
- **SIW mechanisms must provide appropriate ARP/InARP responses (spoof) – ARP Mediation**

Pseudowire Reference Model



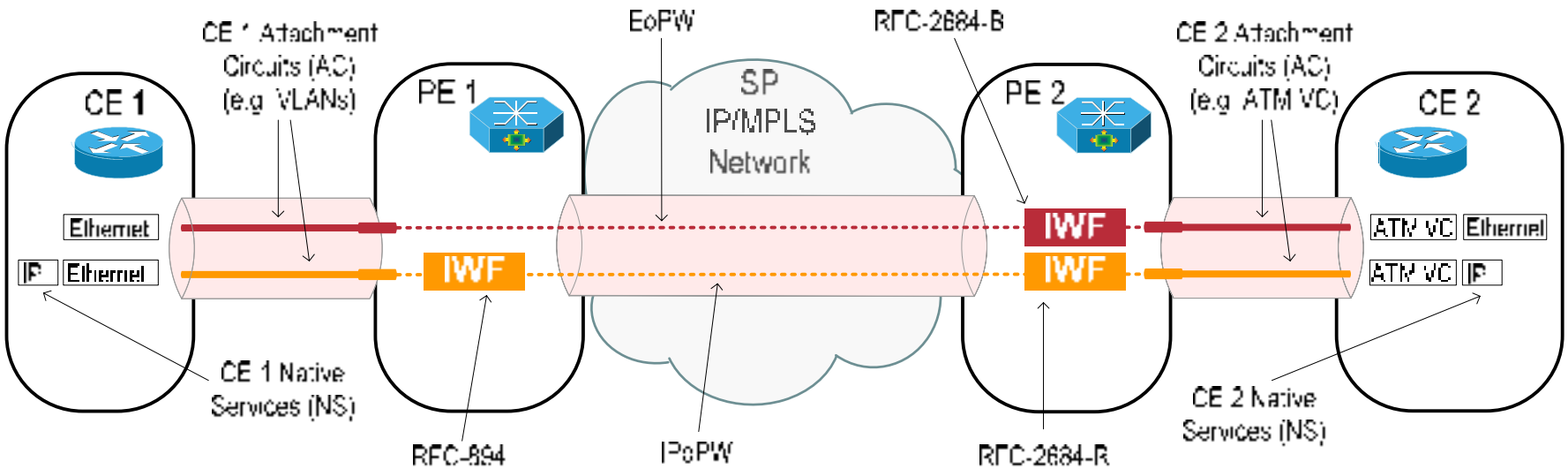
- **Attachment Circuit (AC) is a Virtual Circuit (VC) between a CE and its PE—e.g. ATM VC, FR VC, Ethernet VLAN**
- **Native Service (NS) is the service that gets carried over the AC—e.g. Ethernet, IP, PPP, Multiprotocol**
- **Some examples of NS over AC: Ethernet or IP as NS over an ATM VC, Ethernet or IP over a Frame Relay AC**
- **Service InterWorking comes into play when ACs are different (e.g. ATM and Ethernet)**

Approach to SIW: Local-AC-Termination



- **Attachment Circuits are terminated locally and PW transports only the NS**
- **If AC and NS are the same on one end, then no InterWorking Function (IWF) is required at that node**

SIW Example for Metro Ethernet



- **Two SIW types: Bridged and Routed**
- **Example 1—Bridged SIW (NS = Ethernet):**

  AC1 = Ethernet **AC2 = ATM**

  IWF1 = NULL **IWF2 = RFC-2684-B (obsoleted RFC-1483)**
- **Example 2—Routed SIW (NS = IP):**

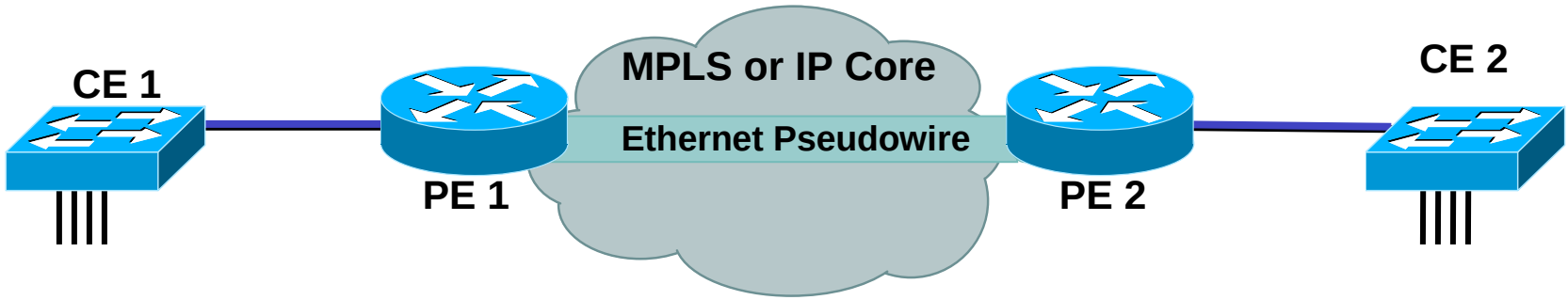
  AC1 = Ethernet **AC2 = ATM**

  IWF1 = RFC-894 **IWF2 = RFC-2684-R (obsoleted RFC-1483)**

Layer 2 Service Inter-Working Features

- Cisco Any Transport Over MPLS (ATOM) and L2TPv3 any-to-any
- Cisco also supports complimentary Layer 2 Service Inter-Working features
  - Integrated Routing and Bridging (IRB)—used at CPE for bridged SIW
  - Route Bridge Encapsulation (RBE)—used at CPE for bridged SIW
  - Bridge Route Encapsulation (BRE)—used at PE for routed SIW (no-IP/MPLS)
- RBE/IRB enables the CPE to encapsulate Ethernet over ATM and FR attachment circuits
  - Ethernet Frame Encapsulated within an ATM RFC2684 Bridged Encapsulation header (RBE or IRB)
  - Ethernet Frame Encapsulated within a FR RFC2427 Bridged Encapsulation header (IRB only)
- BRE terminates RFC2684 Routed Encapsulation ATM PVCs
  - Terminates and Maps multiple PVCs to individual VLANs
  - Inserts/removes an Ethernet MAC header

Ethernet Bridged Service Inter-Working



Native Ethernet

Ethernet VLAN

Bridged Ethernet over ATM

Bridged Ethernet over FR

Bridged Ethernet over HDLC/PPP

Any -2- Any

Native Ethernet

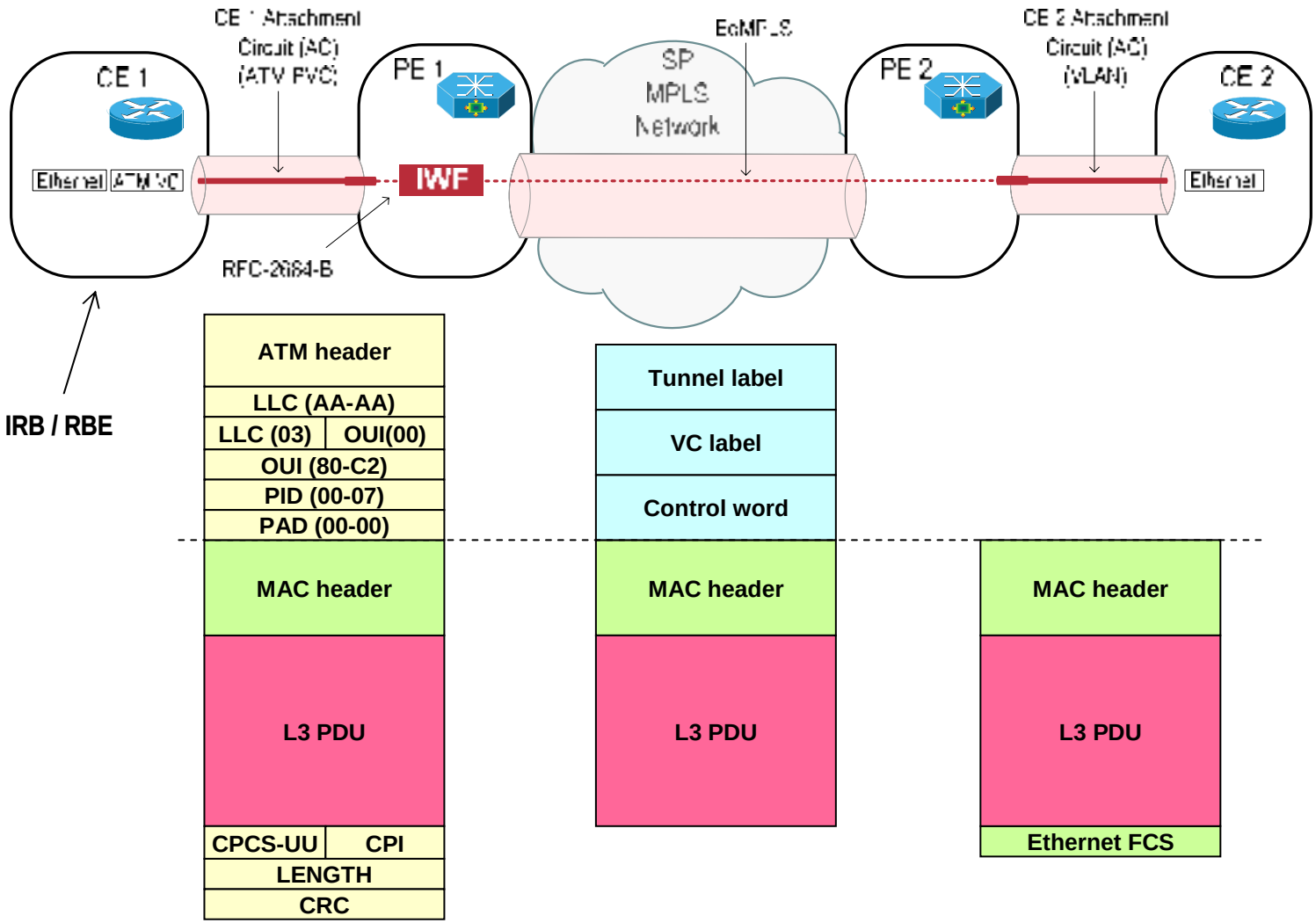
Ethernet VLAN

Bridged Ethernet over ATM

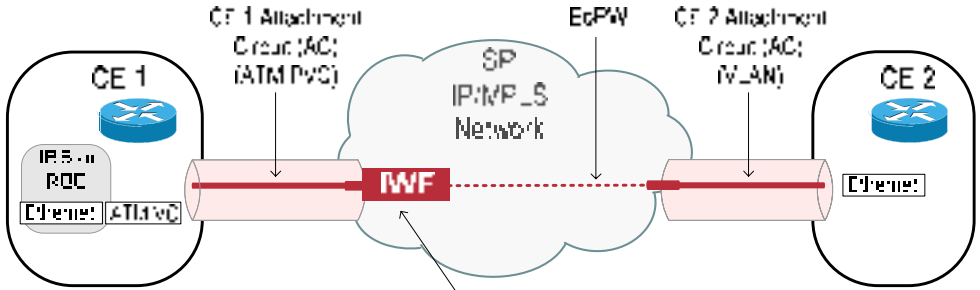
Bridged Ethernet over FR

Bridged Ethernet over HDLC/PPP

Ethernet to ATM AAL5 Bridged SIW



Ethernet to AAL5 Bridged SIW Configuration



CE with RBE

```
interface atm 1/0.1 point-to-point
   encapsulation aal5snap
   ip address 10.0.0.1 255.255.255.0
   pvc 1/100
    atm route-bridge ip
```

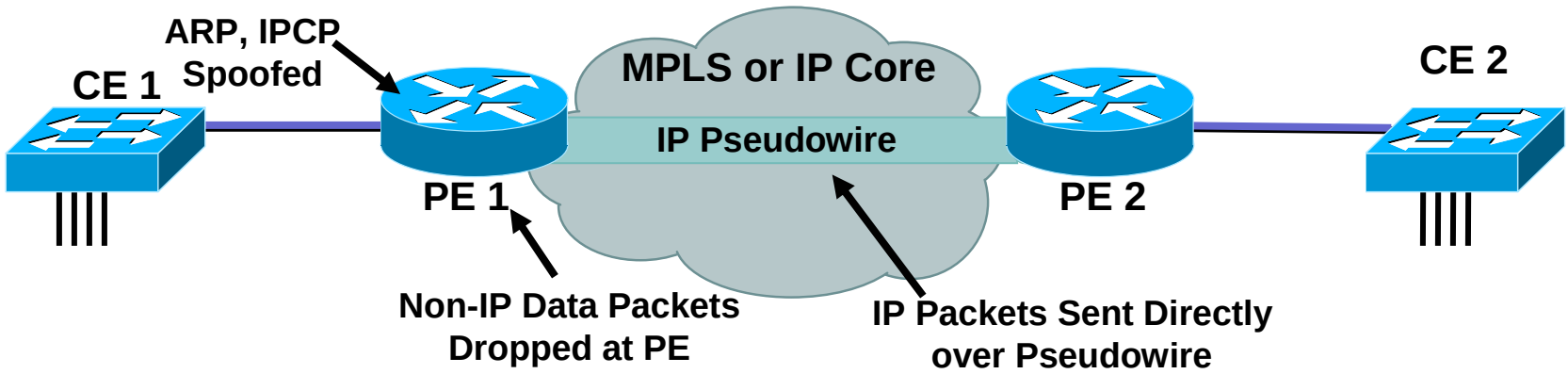
CE with IRB

```
bridge irb
interface atm 1/0.1 point-to-point
   pvc 1/100
     encapsulation aal5snap
   bridge-group 5
!
 interface BVI5
   ip address 10.0.0.1 255.255.255.0
   ip mtu 1500
```

PE

```
pseudowire-class atm-ether
 encapsulation l2tpv3 | mpls
 protocol l2tpv3 | ldp
 interworking ethernet
!
interface atm 1/0.1 point-to-point
  pvc 1/100 l2transport
    encapsulation aal5snap
    xconnect 20.0.0.1 123 pw-class atm-ether
```

IP Routed Service Inter-Working



Ethernet

Frame Relay

PPP/HDLC

ATM

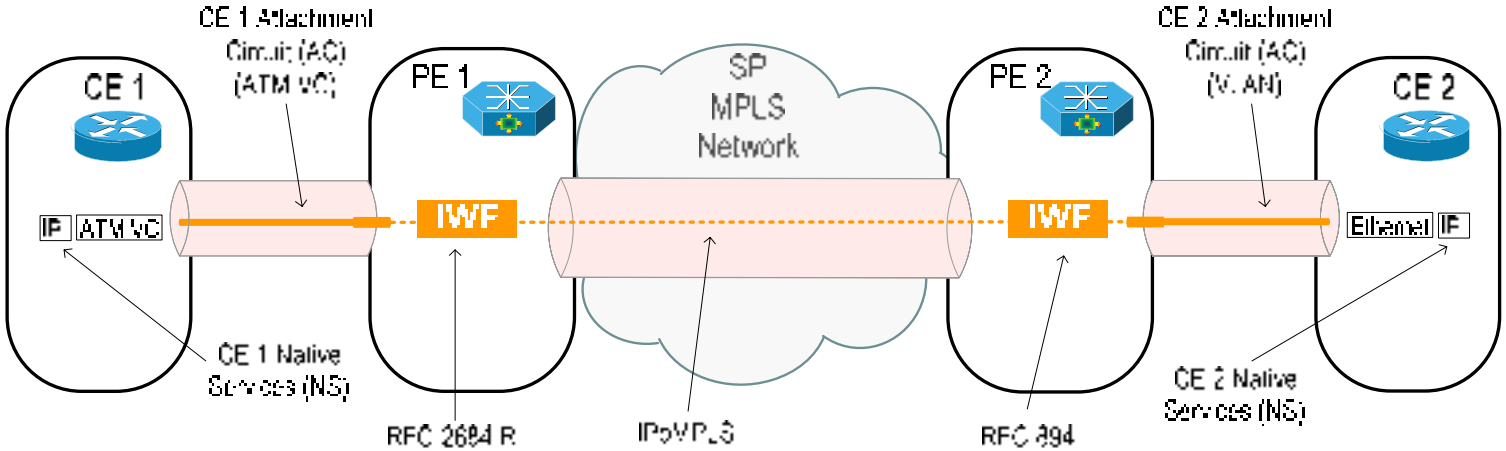
Ethernet

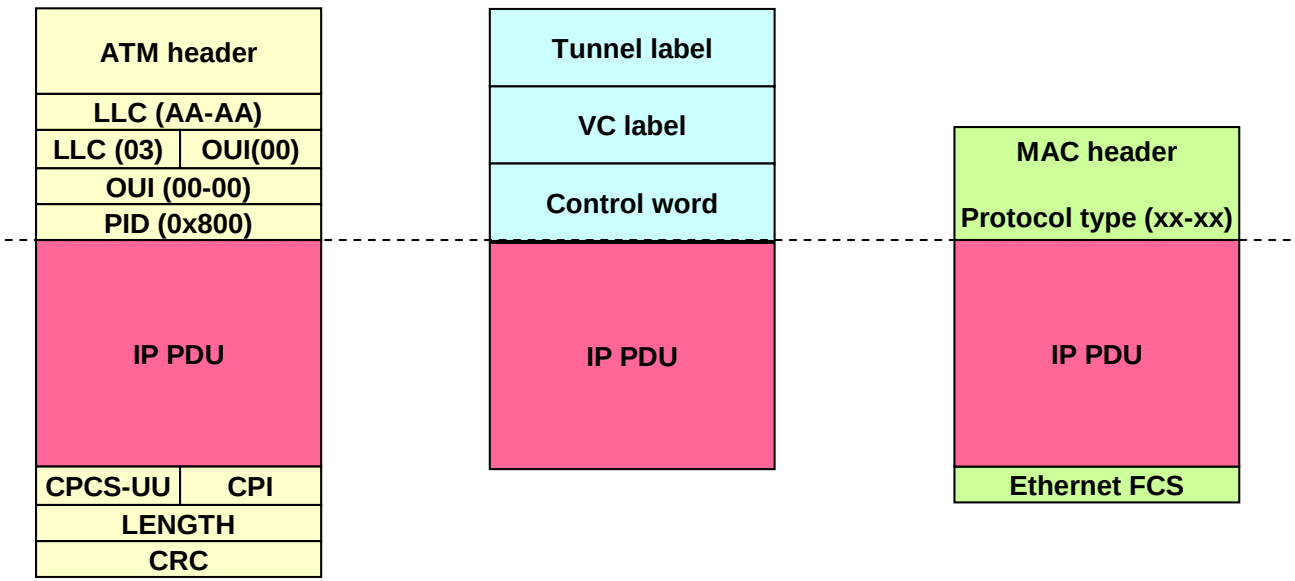
Frame Relay

PPP/HDLC

ATM

Ethernet to ATM AAL5 Routed SIW



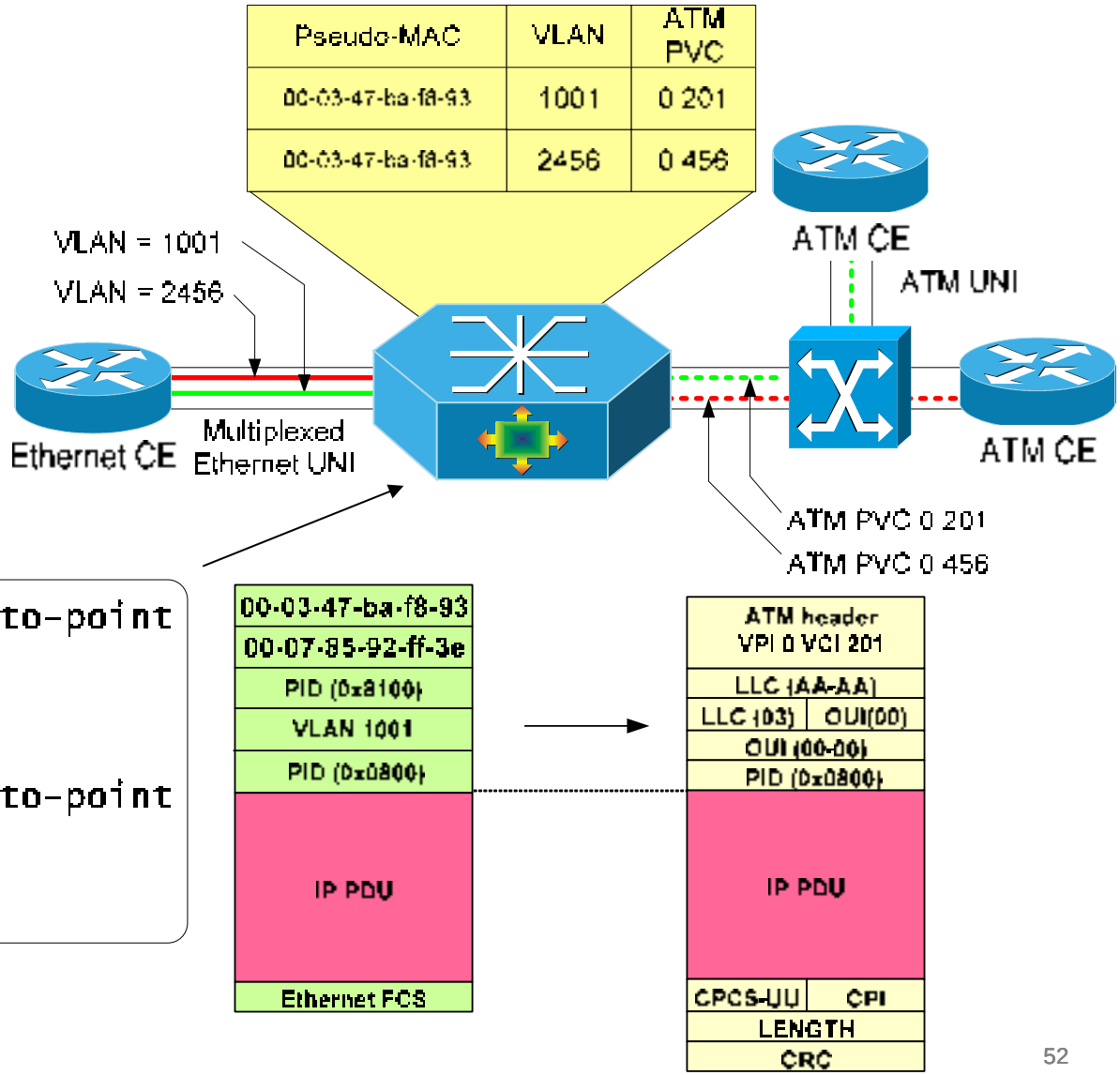


Bridge Route Encapsulation (BRE)

- BRE can be used in a Metro Ethernet Routed SIW scenario without MPLS or IP core
- Terminates RFC2684 routed encapsulation ATM PVCs
- Inserts/removes an Ethernet MAC header for point-to-point services
- Does not require customer configuration changes on ATM CE

Bridge Route Encapsulation (BRE) – Cont.

- **BRE Sample Configuration**



BRE Configuration

```
interface atm 0/0.201 point-to-point
  no ip address
  pvc 0 201
    bre connect 1001

interface atm 0/0.456 point-to-point
  no ip address
  pvc 0 456
    bre connect 2456
```

Routed and Bridged SIW Summary

Cisco.com

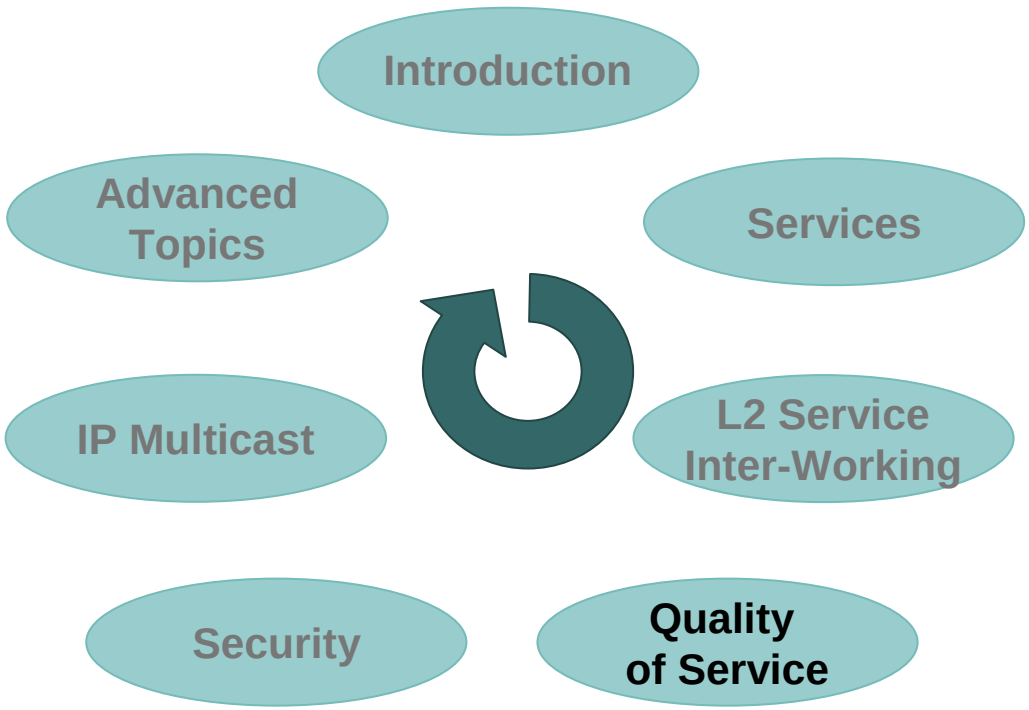
Bridged:

- Native service: Ethernet
- Pro: ARP resolution done by both end CPEs
- Pro: implicit support for any L3 Network protocols
- Cons: ATM/FR CPE has to run in bridging mode, i.e.:
  - IRB for Frame Relay VC attachment circuits
  - RBE or IRB for ATM VC attachment circuit

Routed:

- Native service: IP
- Pro: no configuration changes at ATM/FR CPE
- Cons: ARP resolution/spoofing done at ATM-attached PE (e.g. via BRE)
- Cons: supports one L3 Network Protocol (IP)

Agenda



Why Is QoS Relevant in Metro Ethernet; What SLAs to Expect from an SP

Metro Ethernet End-to-End QoS

- Allows efficient utilization of links that carry voice, video and data
- SP differentiator between service offerings with SLAs
- Customer contracts to an aggregate that contains specific Traffic Classes with Drop, Delay and Jitter attributes
- Sample Traffic Classes – Voice / Interactive Video, Business, Best Effort
- Customer pays for traffic engineered bandwidth not just the access pipe

What Is an SLA?

- **An SLA defines certain attributes about a service**
  - **Availability—4x9s or 5x9s?**
  - **Drop—0.01% or 0.1%?**
  - **Delay—50ms or 100ms?**
  - **Jitter—20ms or 30ms?**
- **The customer application will drive the attributes that are required from the service**
- **A predefined set of SLA attributes can be used by a provider to maximize bandwidth efficiency using statistical gains associated with aggregate flows—Oversubscription**

What SLAs Can I Expect?

- **One SLA per port: Best Effort, CIR, or Voice on a port basis**
- **Multiple SLAs per port: Best Effort, CIR/PIR or Voice on a VLAN basis**
- **Multiple SLAs per VLAN: Best Effort, CIR/PIR or Voice on a Class basis (classified based on L2 COS, IP ToS, outer/inner VLAN)**

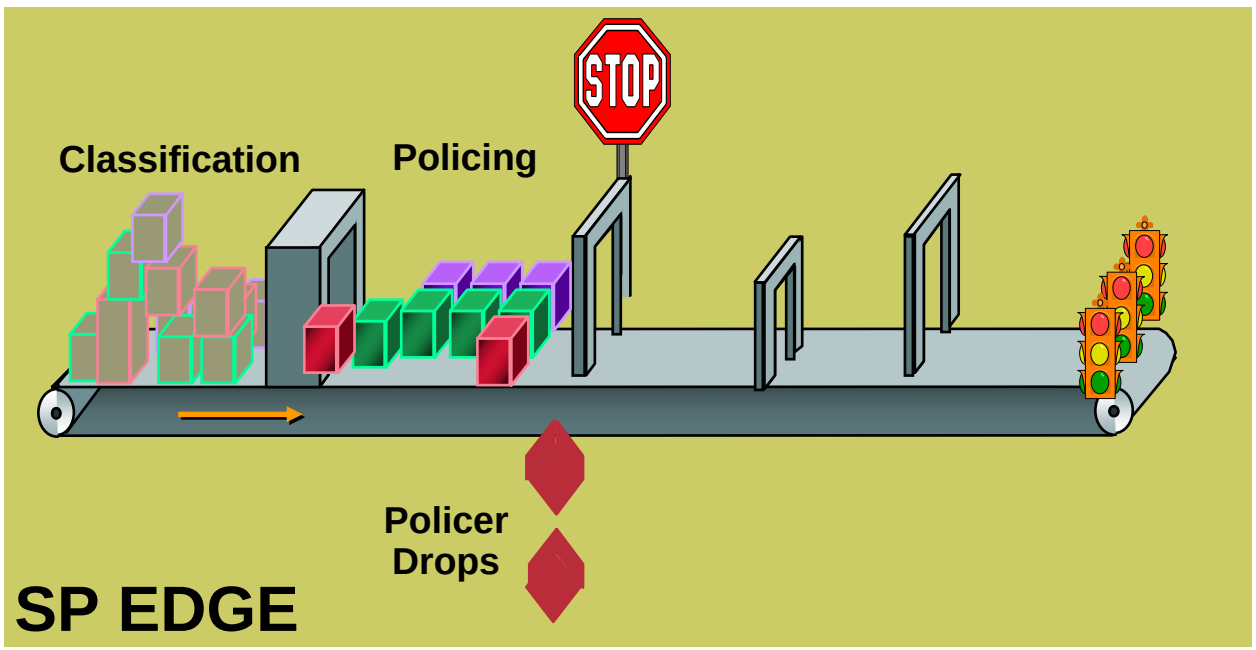
Metro Ethernet End-to-End QoS

- **Point to Point services are commonly enforced (policed) at each ingress point**
  - **What determines SP's lowest speed service?**
  - **Policing not involved for services at port speed (10/100/1000Mbps)—mostly Best Effort**
- **Multipoint services—Point to Cloud model**
  - **Ingress and Egress enforcement**
  - **Most MP2MP services today are Best Effort**
- **SP Bandwidth must be engineered to support SLA classes**

Metro Ethernet End-to-End QoS

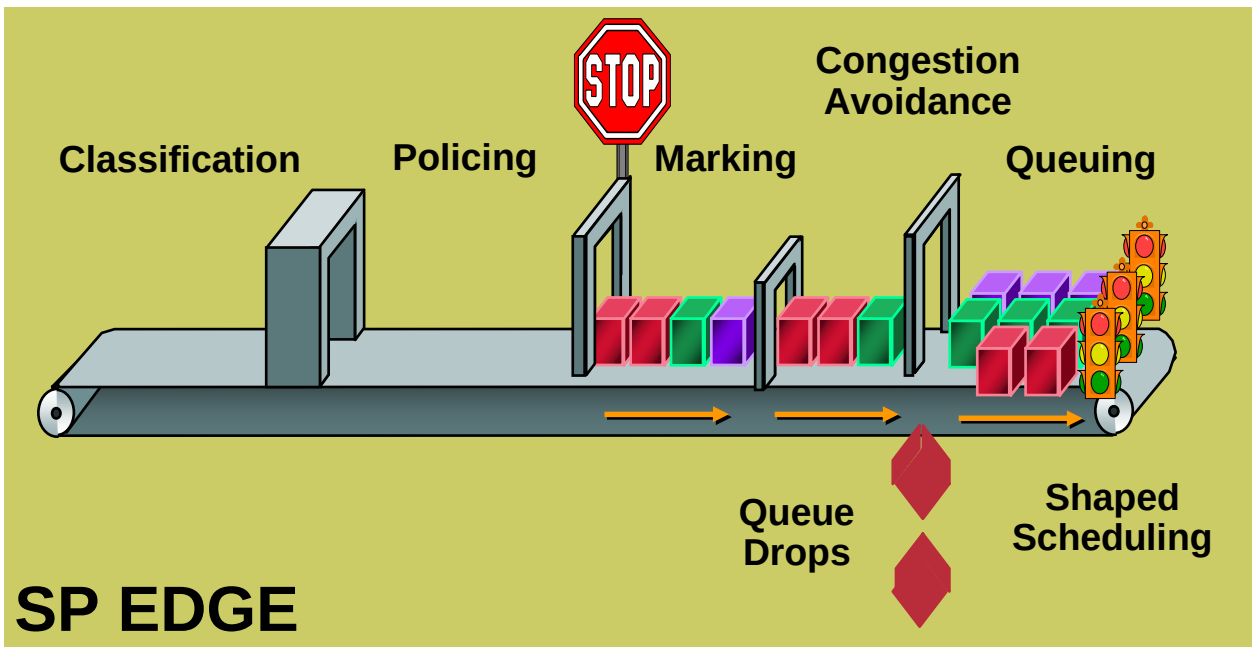
- **Classification based on 802.1p CoS / IP ToS / VLAN or input interface**
- **Ingress Policing at UNI**

  CE should shape whenever possible to maintain application performance

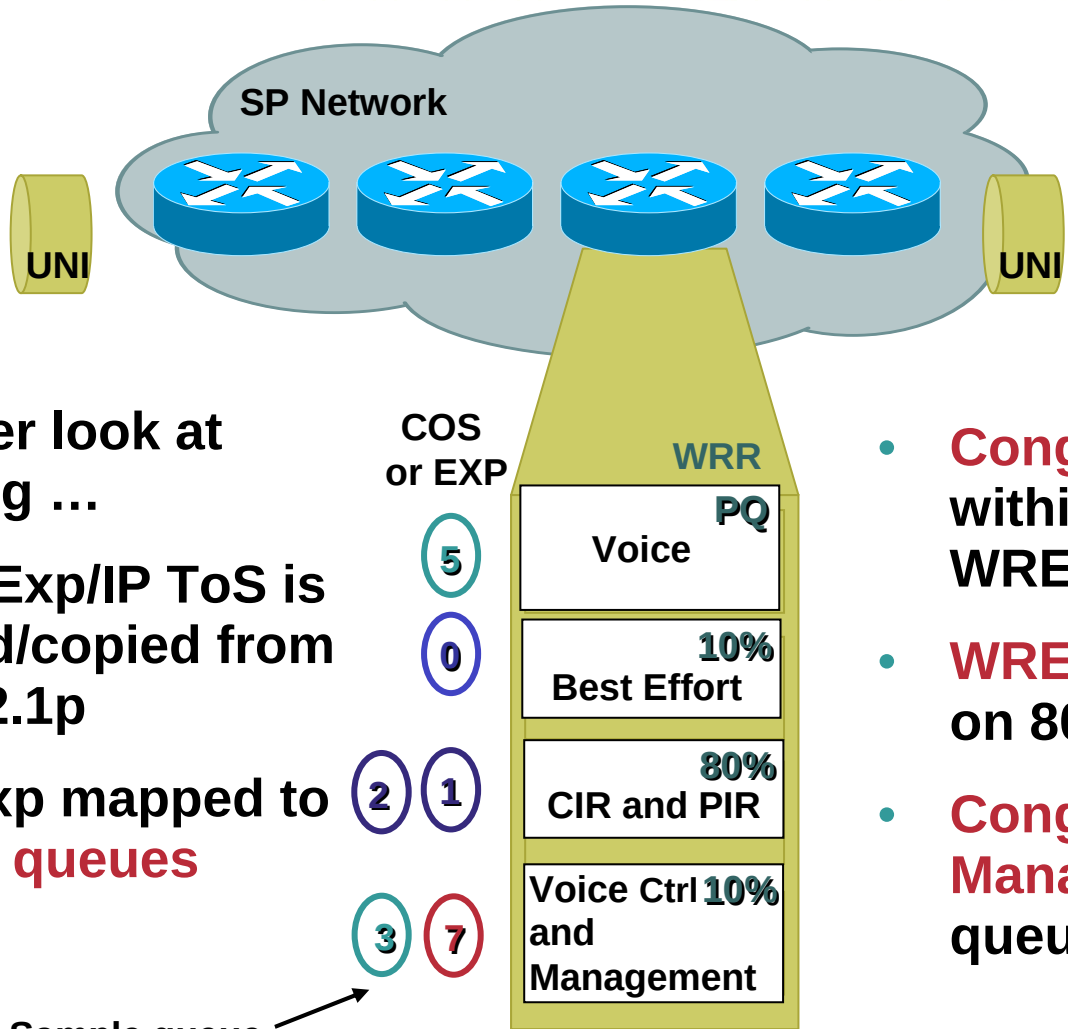


Metro Ethernet End-to-End QoS

- **Marking of 802.1p CoS bits for differentiated SLAs**
- **Customer IP ToS maintained end-to-end**
- **Congestion Avoidance and Egress Queuing throughout the SP network**



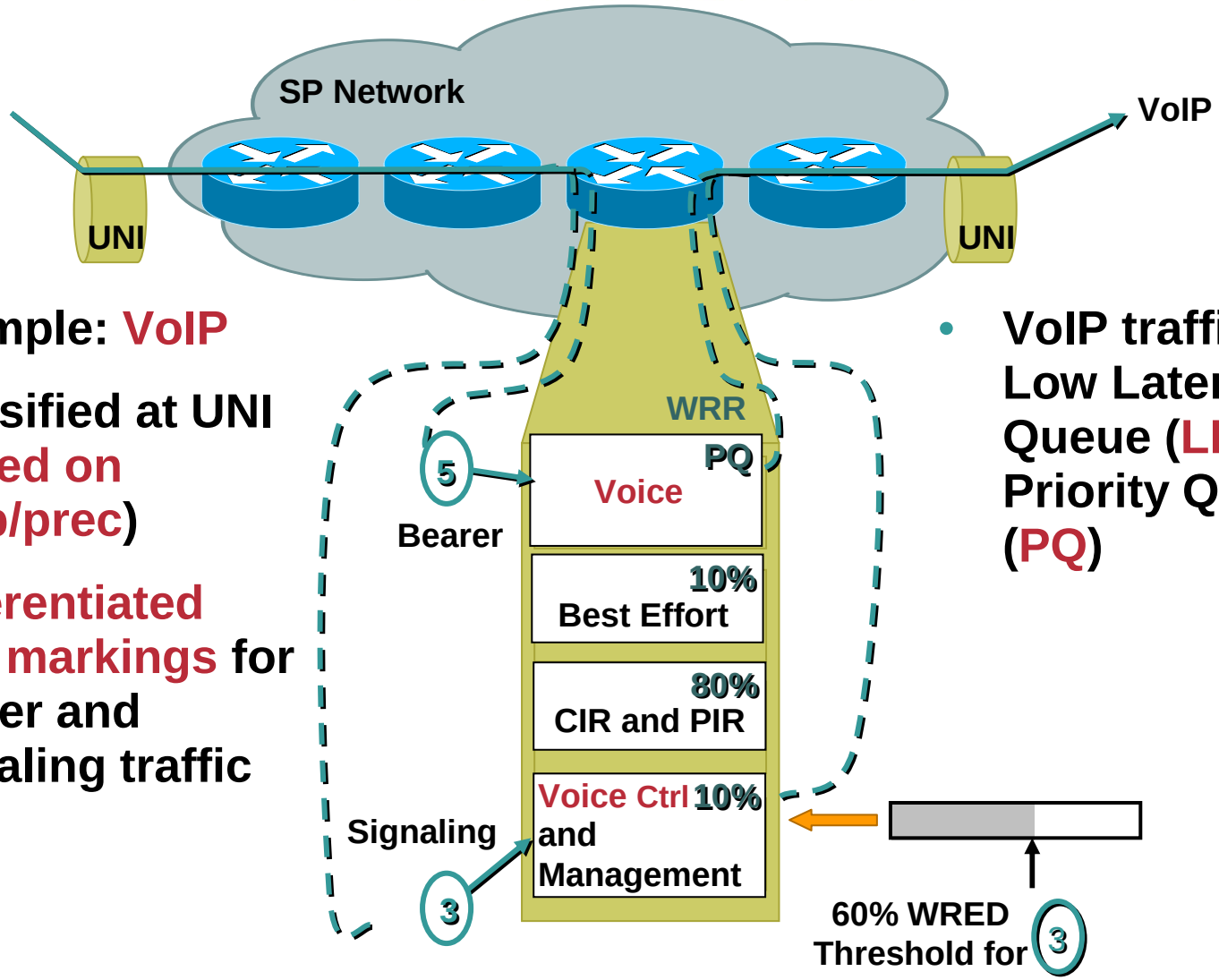
Metro Ethernet End-to-End QoS



- A closer look at queuing …
- MPLS Exp/IP ToS is marked/copied from the 802.1p
- CoS/Exp mapped to egress queues

- Congestion Avoidance within a queue (e.g. WRED)
- WRED thresholds based on 802.1p / EXP
- Congestion Management among queues (e.g. WRR)

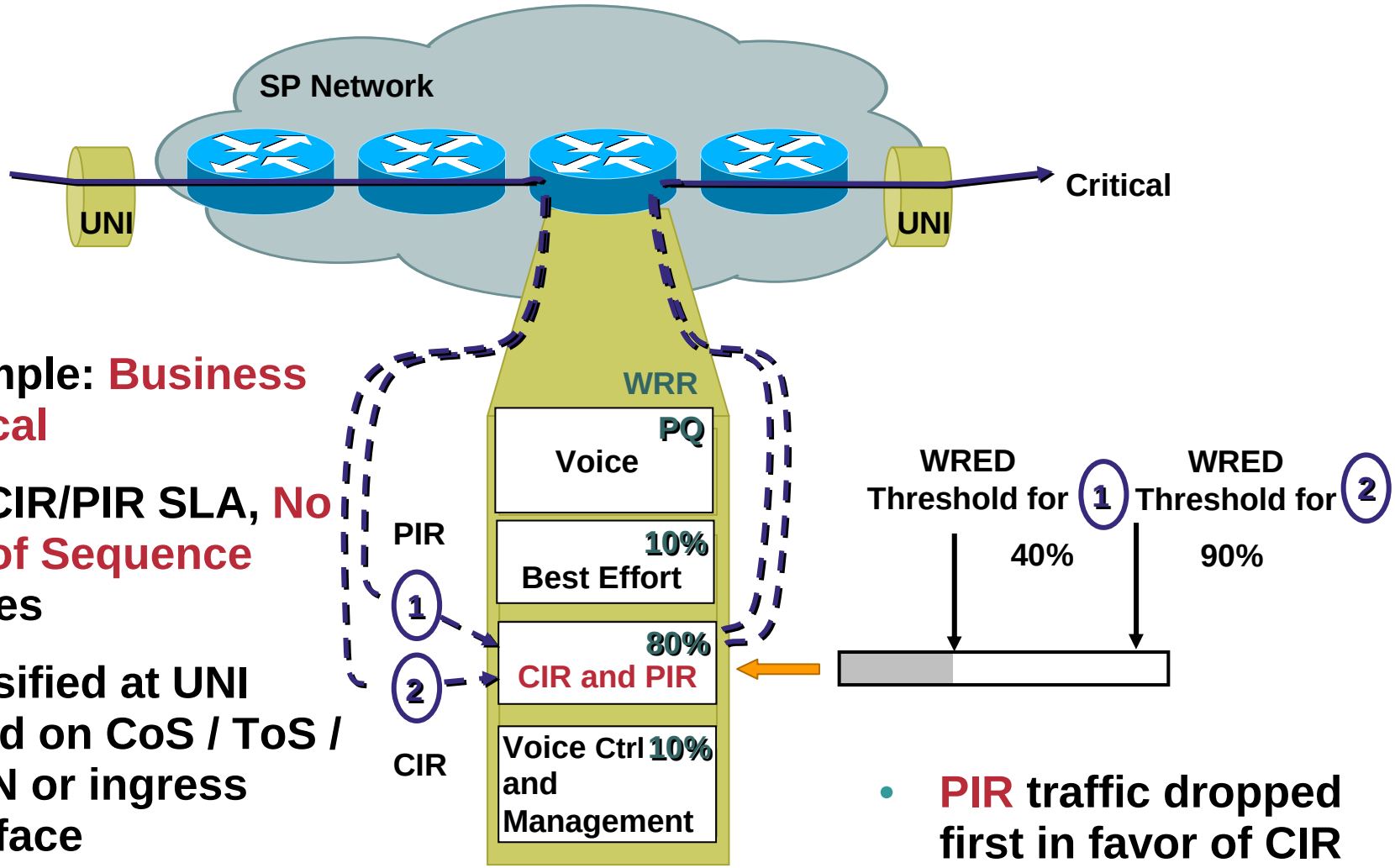
Metro Ethernet End-to-End QoS



- Example: VoIP
- Classified at UNI (based on dscp/prec)
- Differentiated CoS markings for bearer and signaling traffic

- VoIP traffic sent to Low Latency Queue (LLQ) or Priority Queue (PQ)

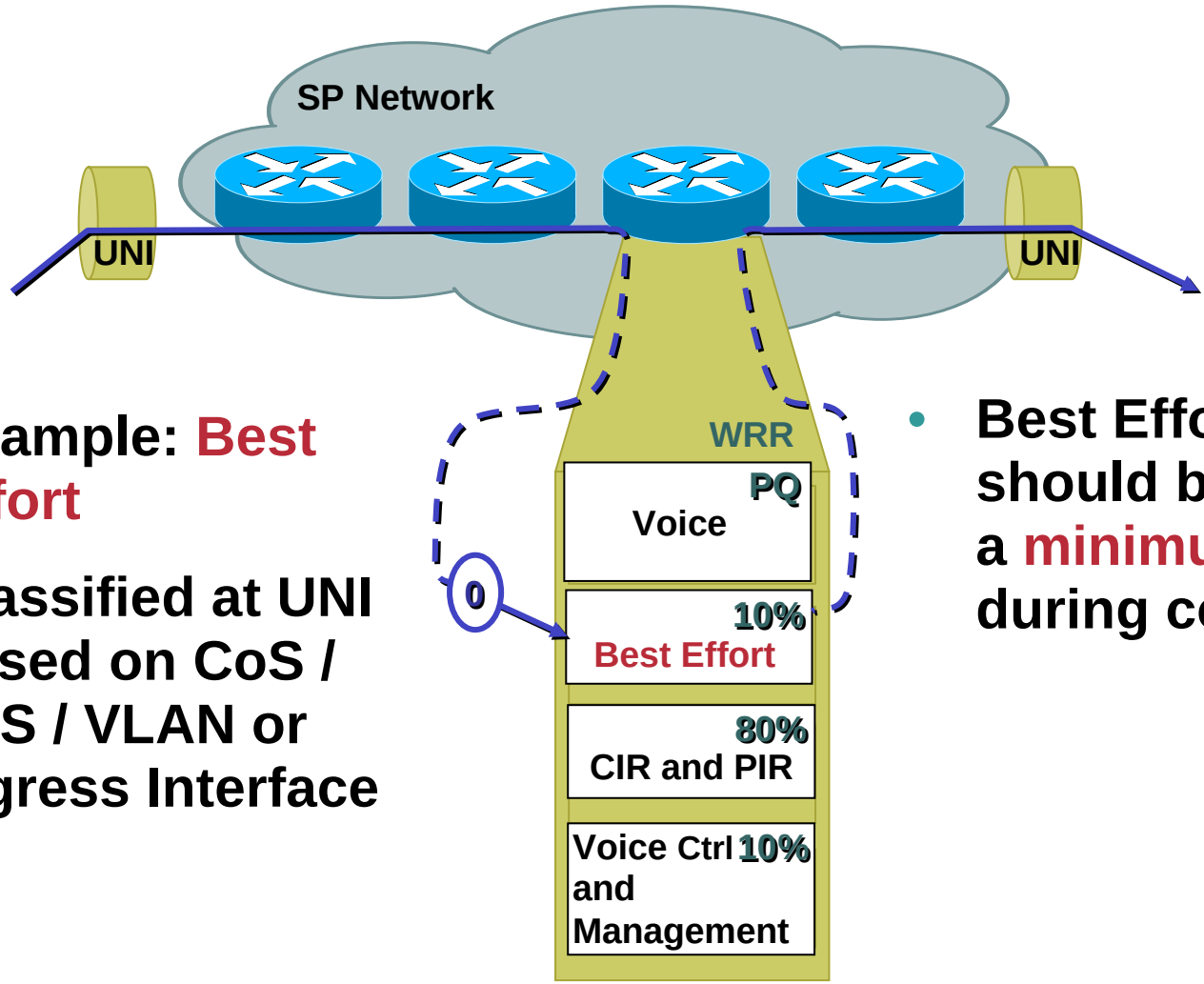
Metro Ethernet End-to-End QoS



- Example: Business Critical
- For CIR/PIR SLA, No Out of Sequence frames
- Classified at UNI based on CoS / ToS / VLAN or ingress Interface

- PIR traffic dropped first in favor of CIR

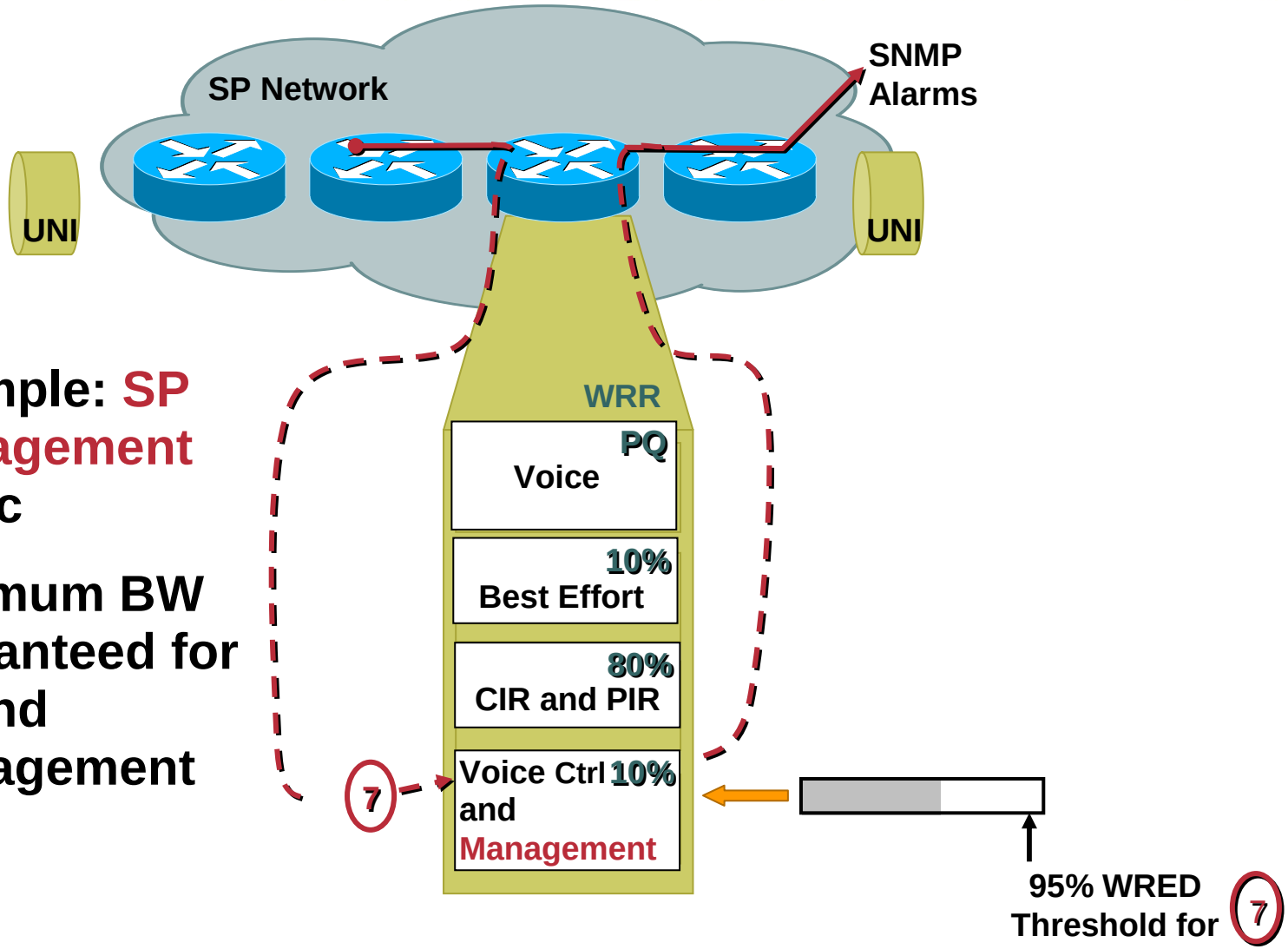
Metro Ethernet End-to-End QoS



- Example: Best Effort
- Classified at UNI based on CoS / ToS / VLAN or ingress Interface

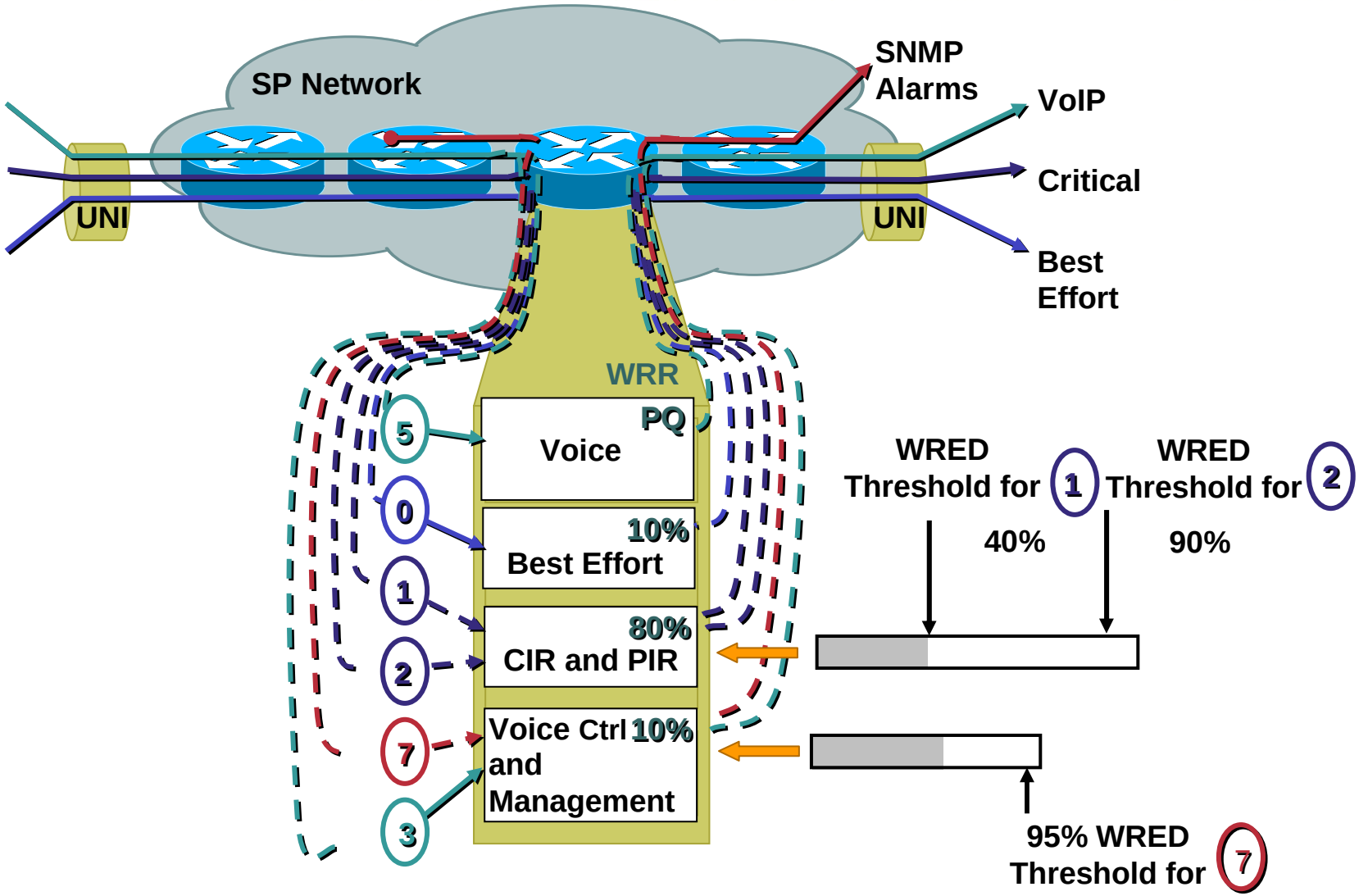
- Best Effort traffic should be assigned a minimum BW during congestion

Metro Ethernet End-to-End QoS



- Example: SP Management traffic
- Minimum BW guaranteed for inband management

Metro Ethernet End-to-End QoS



Metro Ethernet End-to-End QoS

- **Ethernet QoS similar to ATM/FR model**

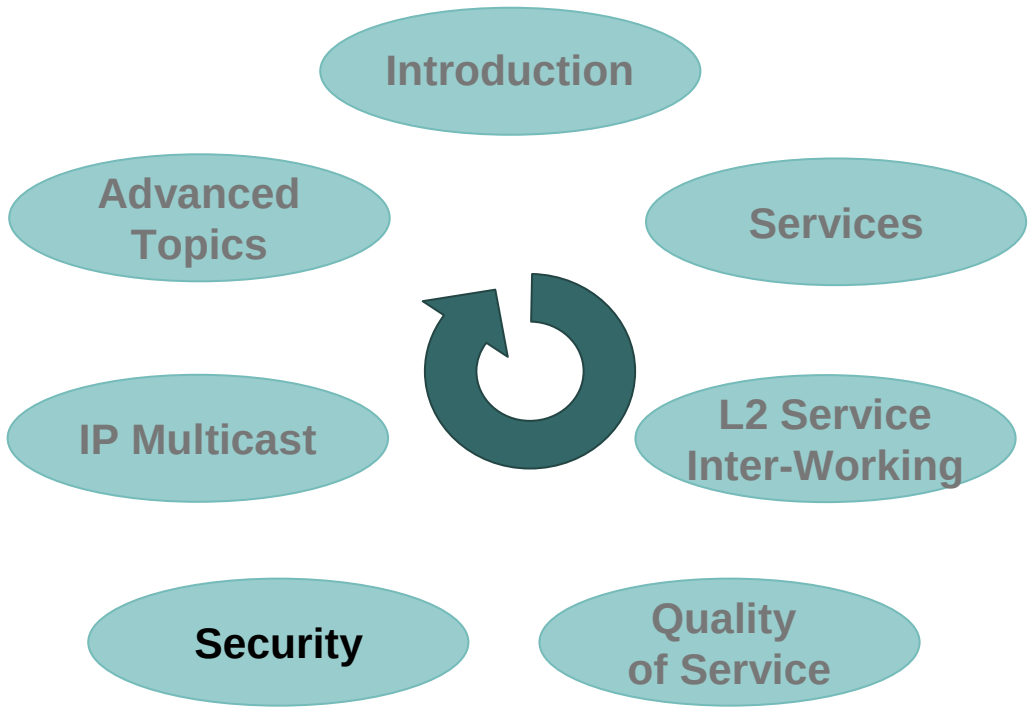
  CIR/PIR is well accepted today

- **Migration to DSCP-like model that can be applied to Layer 2 and Layer 3 services**

  CIR/PIR can be extended to other QoS models allowing for tiered bandwidth rates, i.e. Voice, Business and Best Effort traffic classes

- **Consistent QoS model for L2 and L3 VPNs**

Agenda



How to Secure an Enterprise Network Connected to a Metro Ethernet Provider

Ethernet Security

- **Security is a prime consideration within any public switched network**
  - **One user should not affect any other user**
- **Ethernet as a technology could be insecure due to its "plug and play" nature**
- **With little knowledge, an Ethernet switched access network can be exploited**

Ethernet Security

- Attacks such as dSniff exploit Ethernet weaknesses

  http://naughty.monkey.org/~dugsong/dsniff/

  dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, and webspy

  arpspoof, dnsspoof, and macof

  sshmitm and webmitm

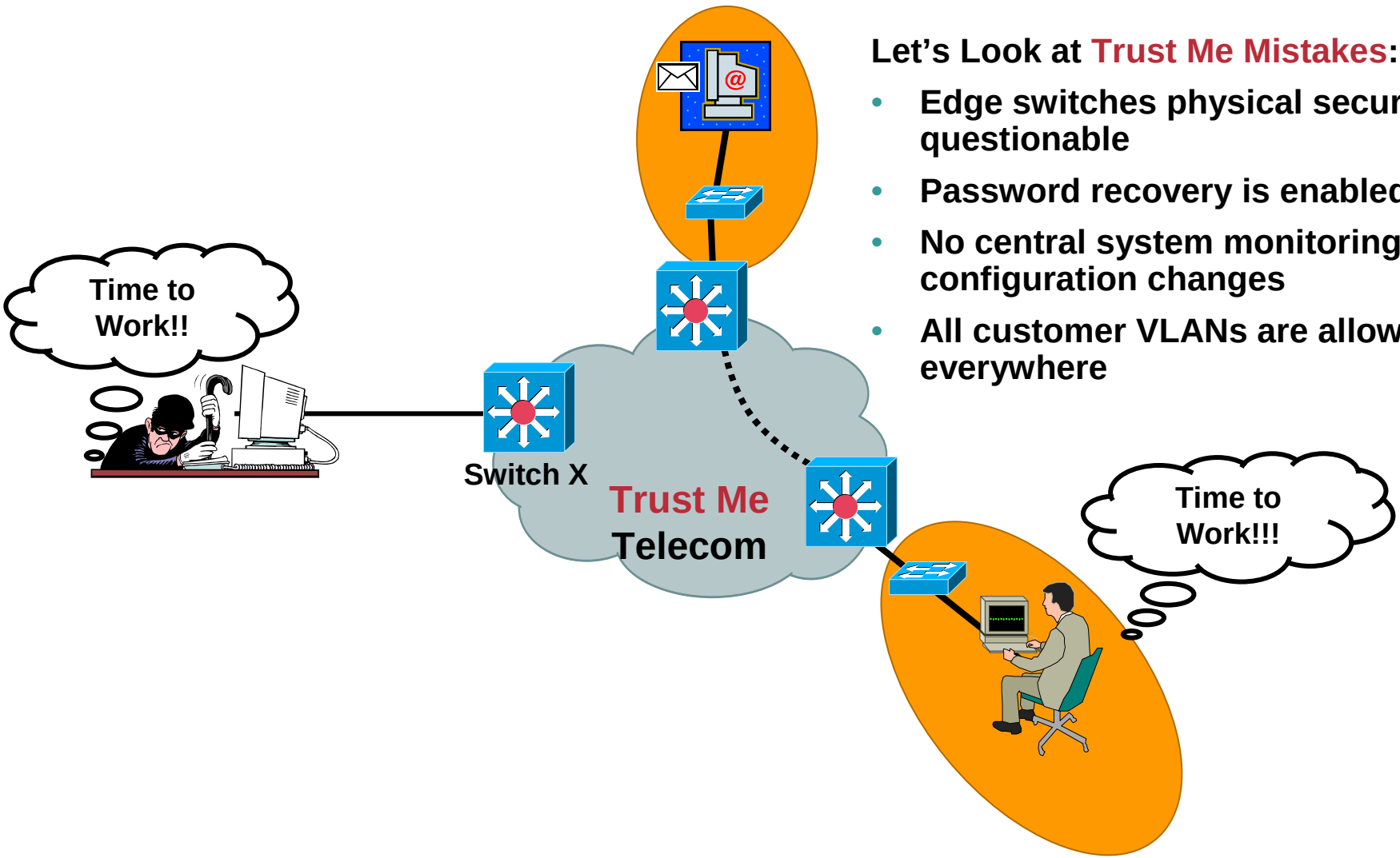
- This tool and others exploit Ethernet technologies and its mechanisms to gain access to information

  ARP Spoof/MAC Flooding/SSH-SSL Interception/ Selective Sniffing

- Other exploits can be used to launch DOS attacks

  802.1D/w/s Spanning Tree can be hijacked

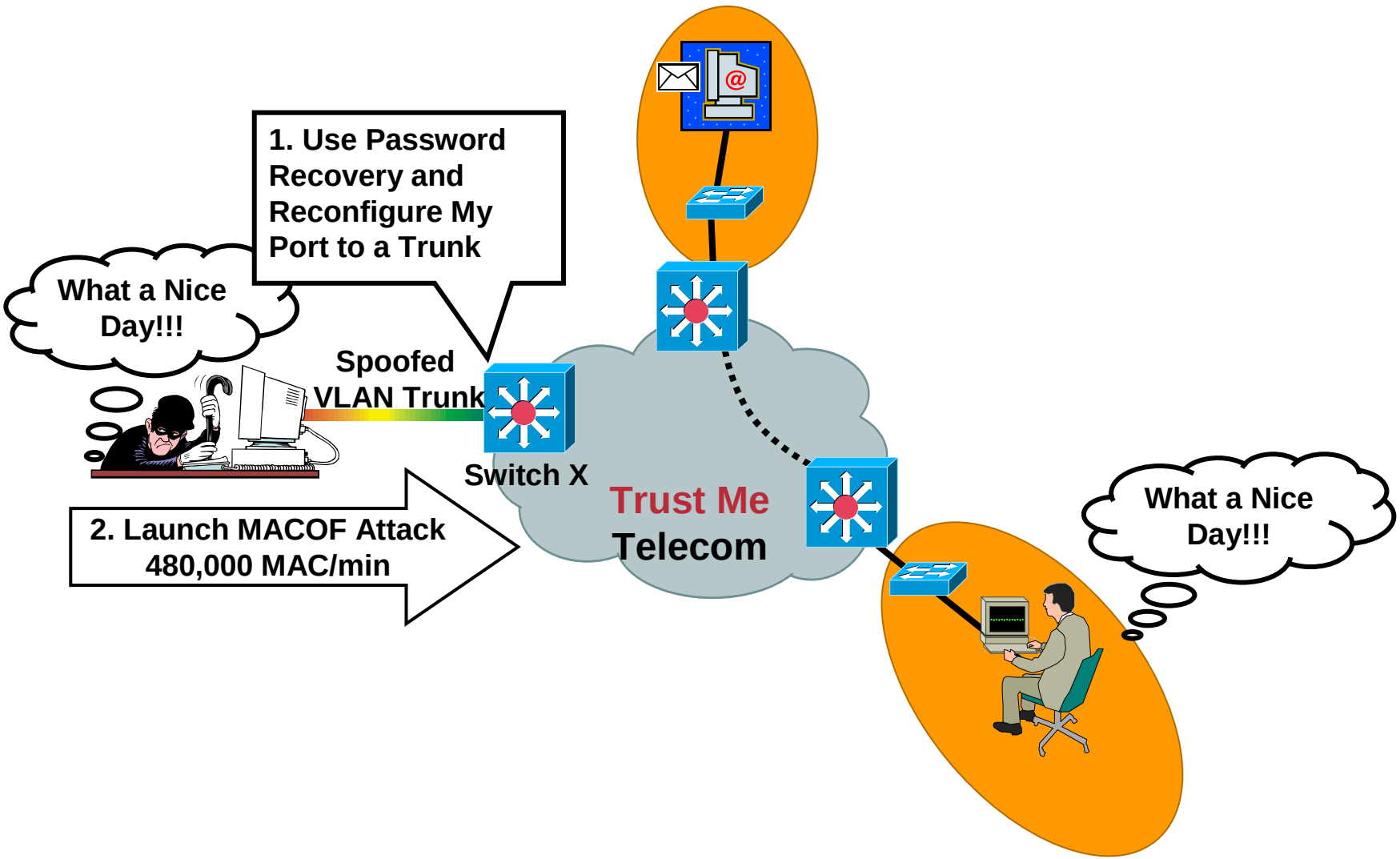
Ethernet Security: An Example of What Can Go Wrong



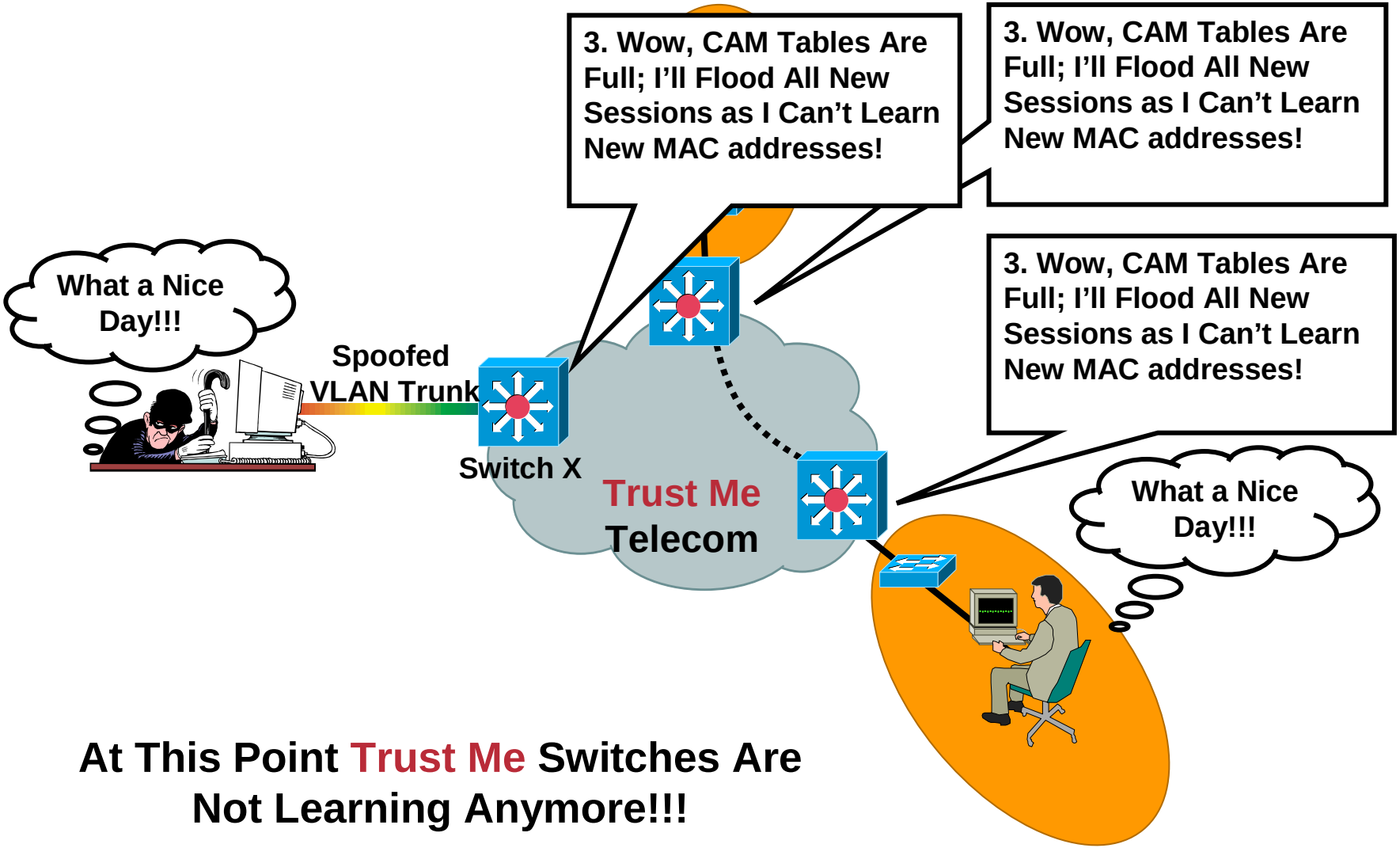
Let's Look at Trust Me Mistakes:

- **Edge switches physical security questionable**
- **Password recovery is enabled**
- **No central system monitoring for configuration changes**
- **All customer VLANs are allowed everywhere**

Ethernet Security: An Example of What Can Go Wrong

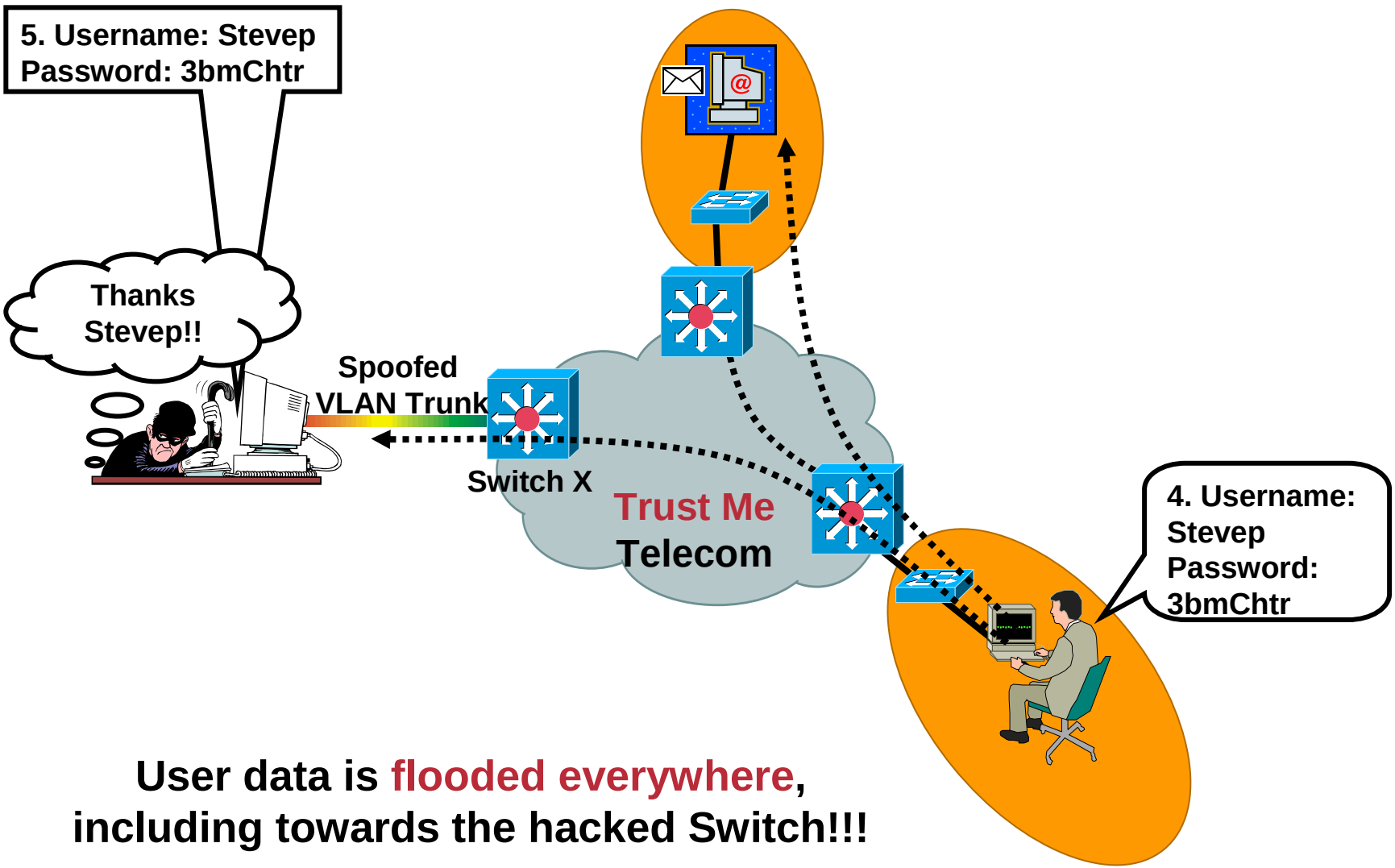


Ethernet Security: An Example of What Can Go Wrong



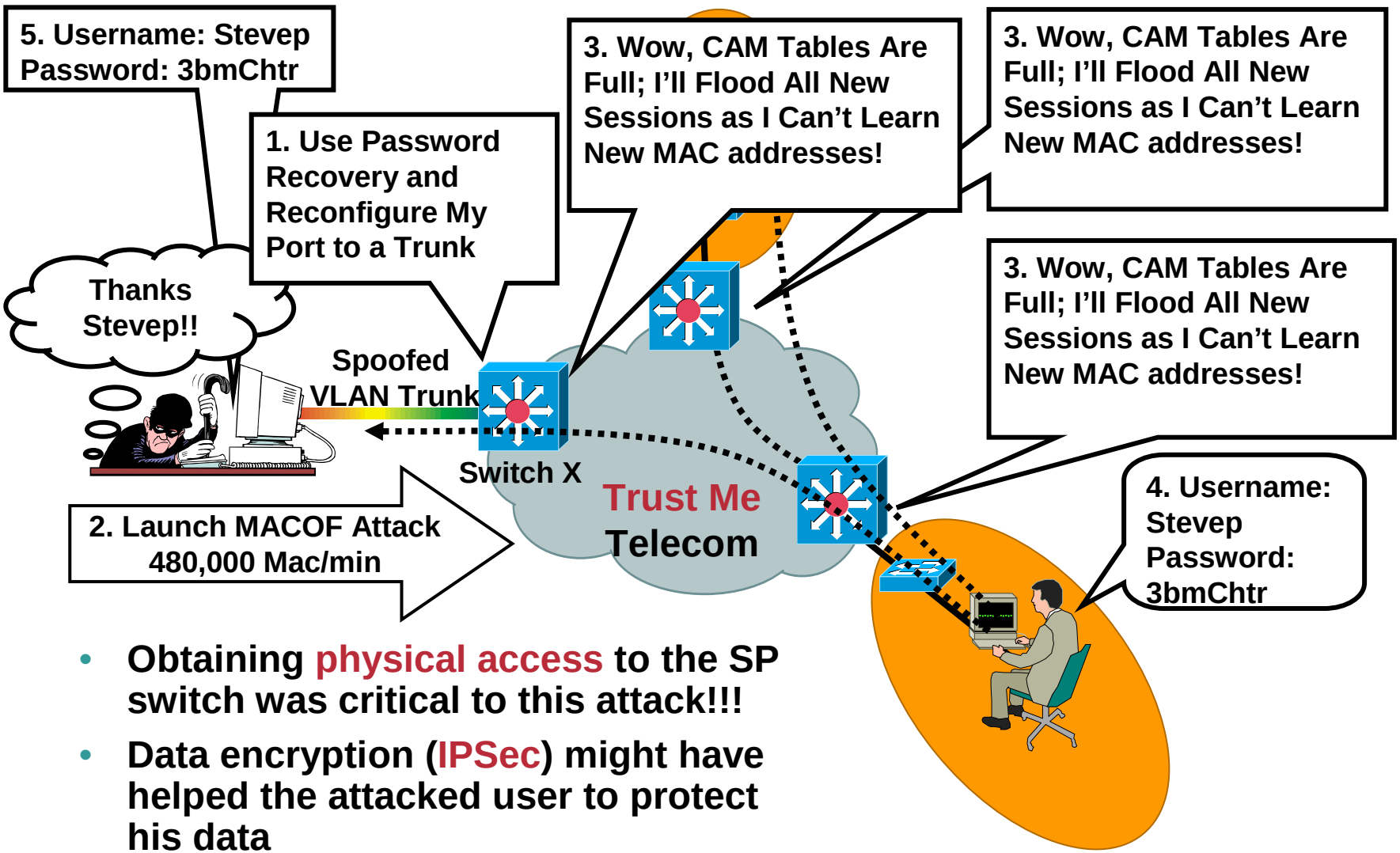
At This Point Trust Me Switches Are Not Learning Anymore!!!

Ethernet Security: An Example of What Can Go Wrong



User data is flooded everywhere, including towards the hacked Switch!!!

Ethernet Security: An Example of What Can Go Wrong



- Obtaining physical access to the SP switch was critical to this attack!!!
- Data encryption (IPSec) might have helped the attacked user to protect his data

Ethernet Security: What Can I Do to Secure My Network?

- **Now we understand what can go wrong, we can identify what we can do to fix it**
  1. **Secure your routers or switches**
  2. **Secure your control protocols**
  3. **Secure your communications**
  4. **Track and log everything**

Ethernet Security:
#1. Secure Your Routers or Switches

- Use RADIUS or TACACs

  Authenticate, Authorize and Audit

- Use SSH instead of Telnet

  Encrypts all communications

- Use good passwords

  Use upper and lower case and numbers

- Change SNMP community strings

  Treat them like root passwords

Ethernet Security: #1. Secure Your Routers or Switches (Cont.)

- Implement IP access filters for SNMP access
- Disable Dynamic Trunking protocol (DTP) on edge switches
  - Allowed only required VLANs
- Physical access will also be an issue
- Disable TCP and UDP-small-servers

Ethernet Security: #2. Secure Your Control Protocols

- IEEE 802.1D Spanning Tree BPDUs are not encrypted
- Consider IEEE 802.1s where Spanning Tree BPDUs are encrypted
- To prevent hijack of Spanning Tree consider RootGuard and BPDUGuard

Ethernet Security:
#2. Secure Your Control Protocols (Cont.)

- Use passwords for protocols such as VTP
- Disable CDP

  CDP advertises information that can be used in a DOS attack (IP address, Cisco IOS version)

- Secure routing protocols using passwords and MD5 Authentication

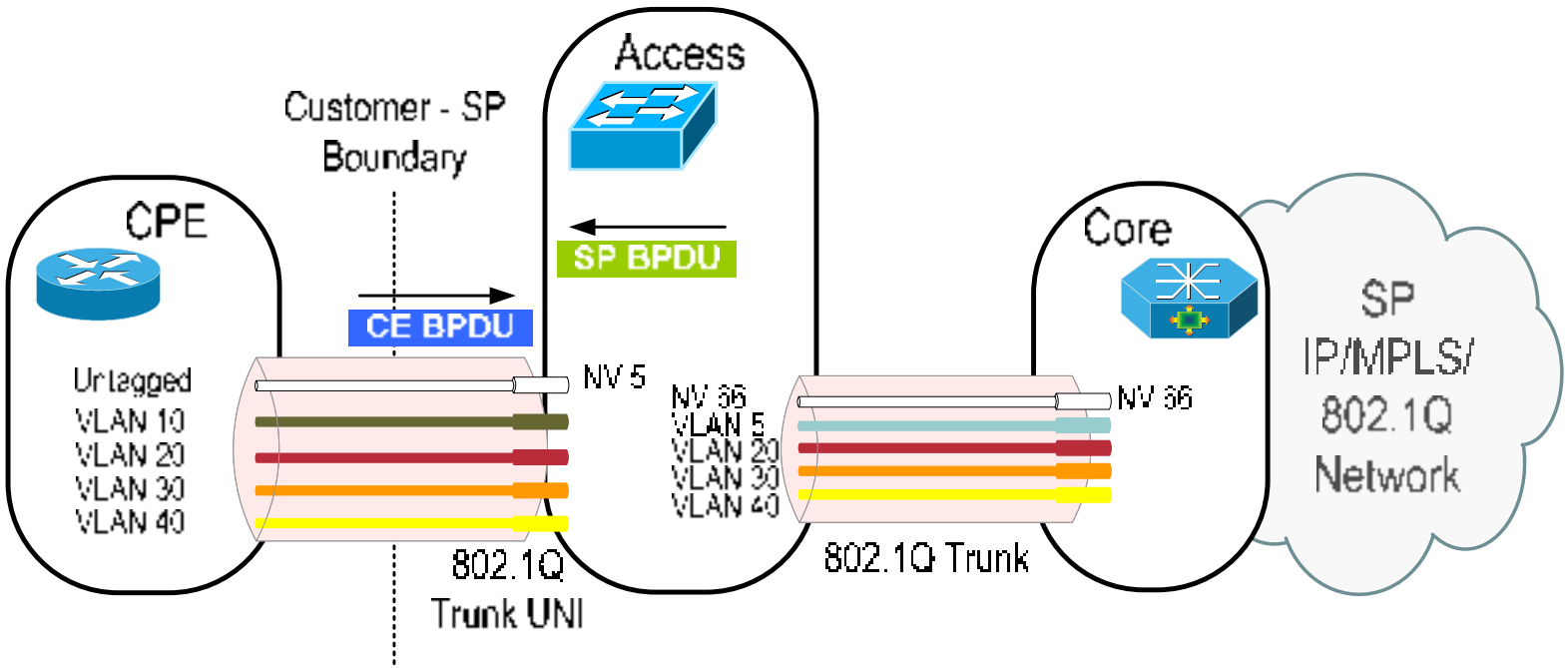
Ethernet Security: #3. Secure Your Communications

- Implement IEEE 802.1x to validate user identity
- Configure Port Security on the UNIs
- Use Firewall and IDS to protect important devices
  - Protect DNS/DHCP/WINS servers
- Use IPSec to encrypt sensitive data
  - Use IPSec between routers connected to public service
  - Use IPSec VPN and one time keys for mobile workers

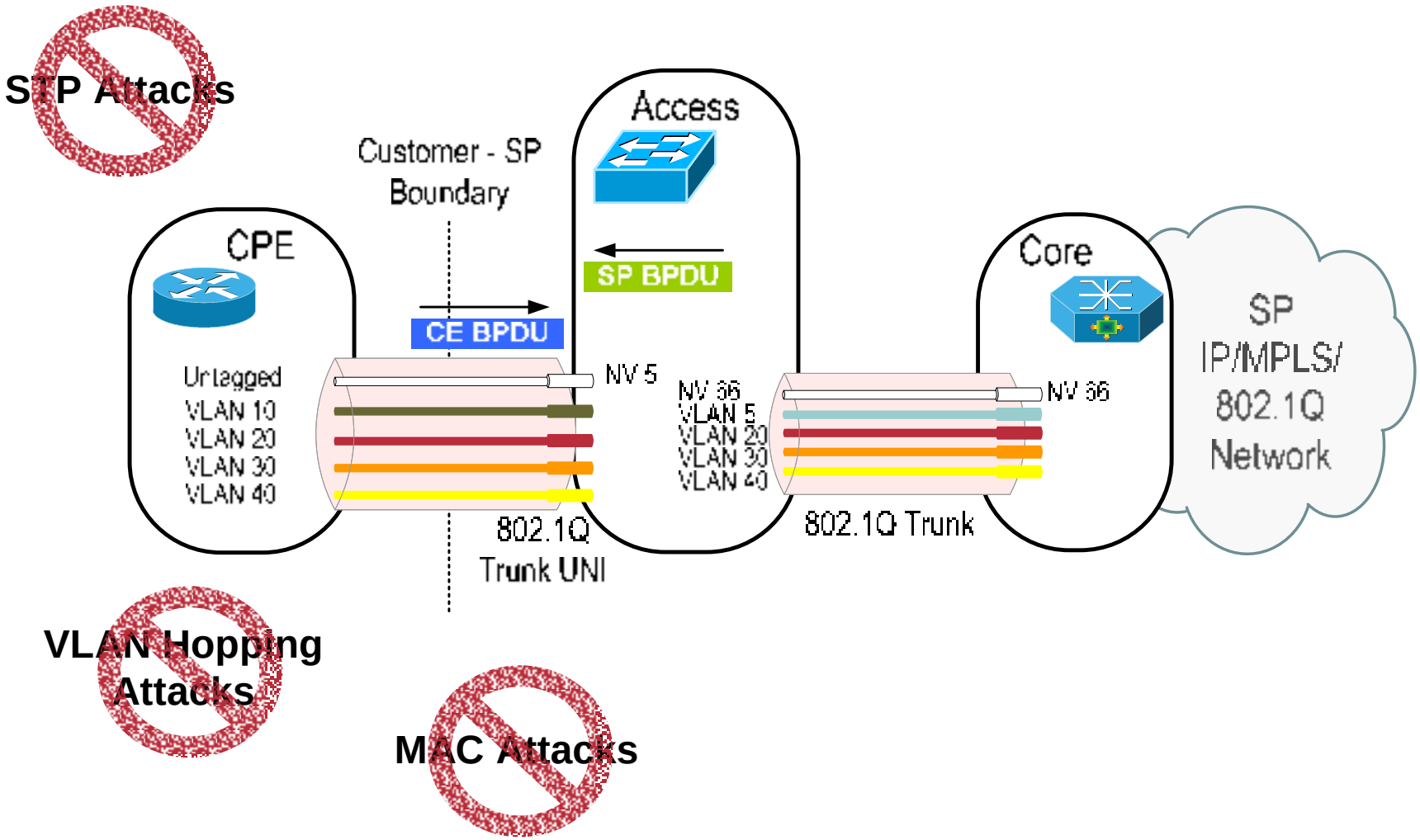
Ethernet Security: #4. Track and Log Everything

- Log Routing protocol adjacency changes
  - It may be an unauthorized device?
- Track interface changes (up/down)
  - It may point to a device that has been password recovered
- Track Configuration changes
  - Was the configuration change known and authorized?
  - Did the change occur after a power cycle?
- Track Firewall and IDS violations
  - It may identify an attack?
- Maintain an audit trail for analysis

Ethernet Security: SP Recommendations

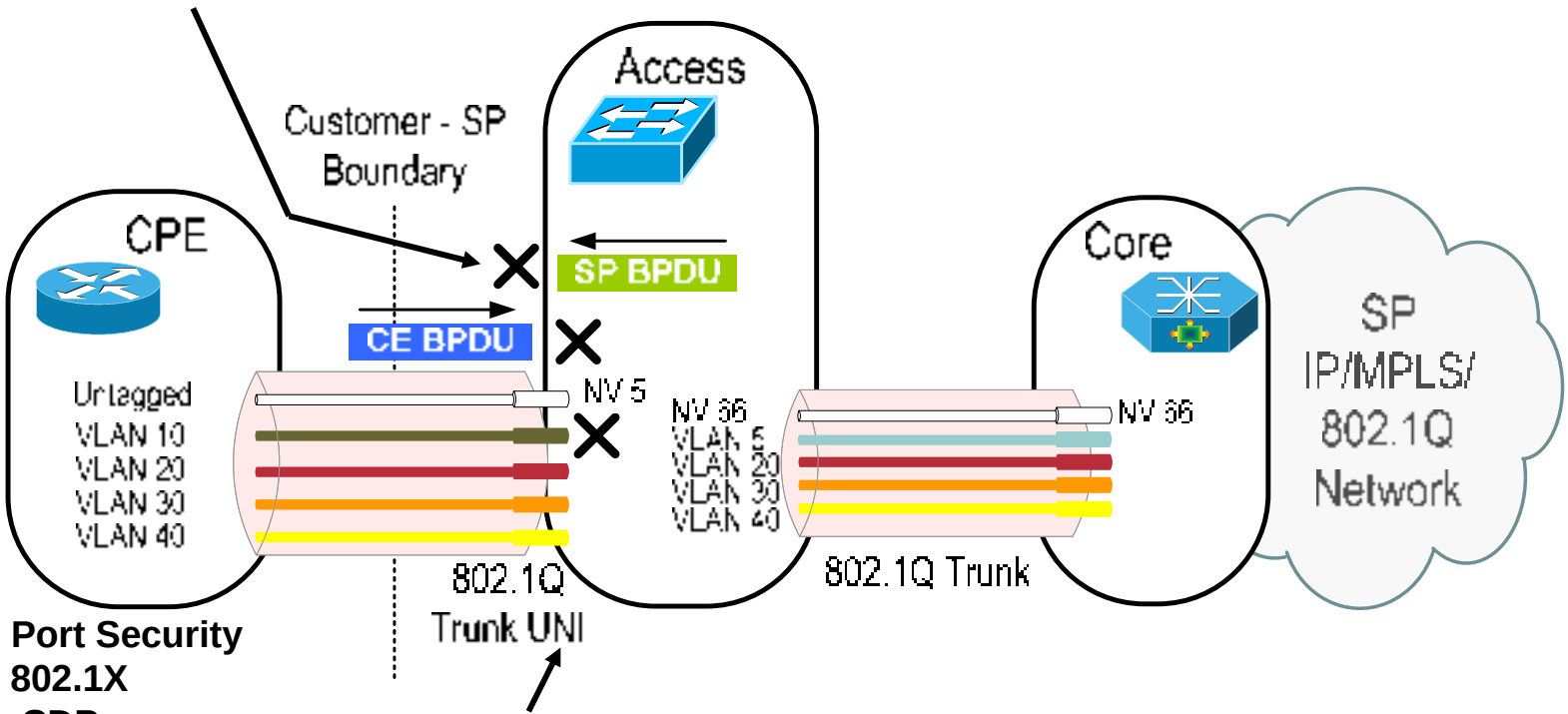


Ethernet Security: SP Recommendations



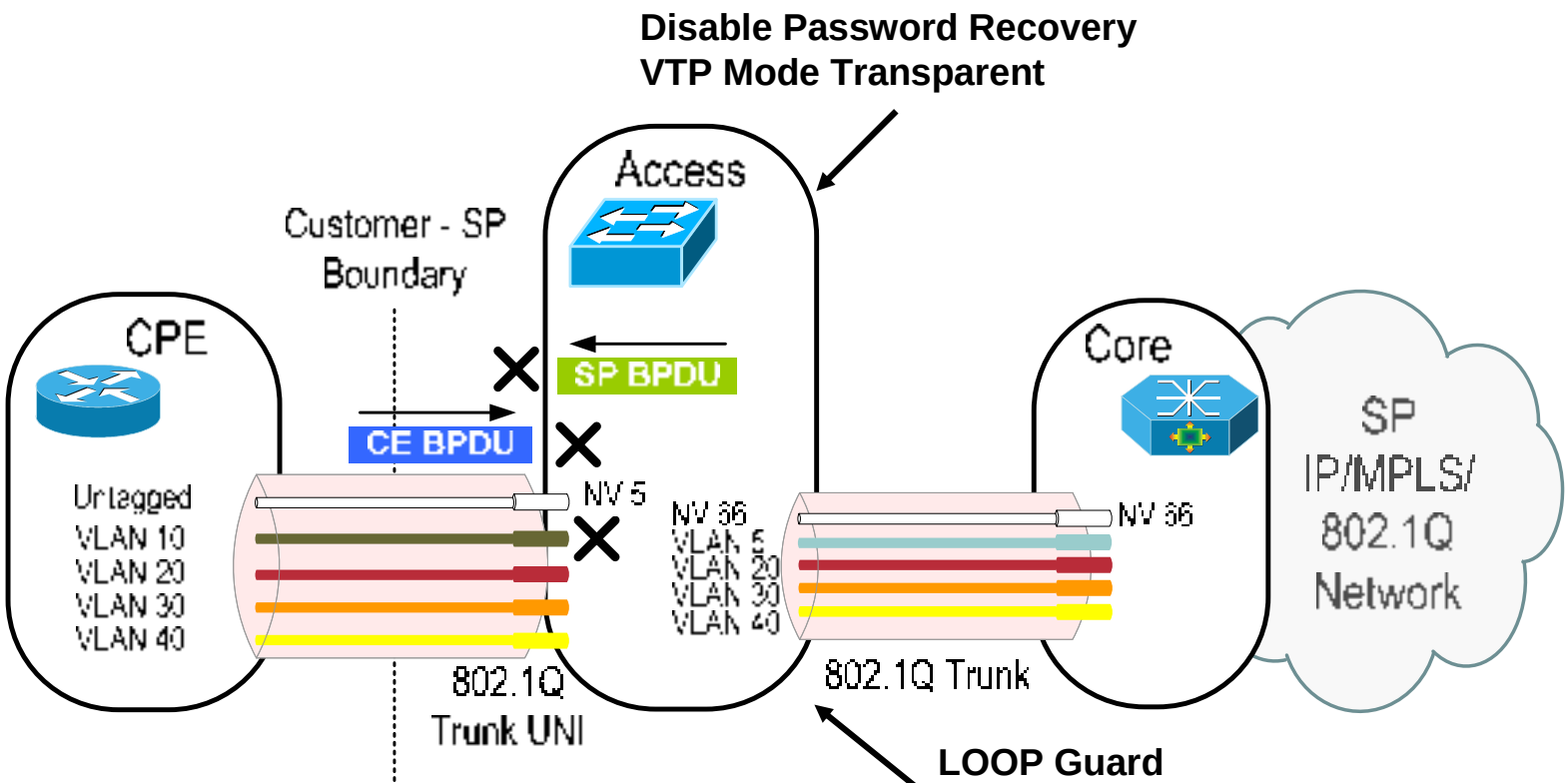
Ethernet Security: SP Recommendations

BPDU Filter (for Egress SP BPDU)
MAC ACLs (for Ingress CE BPDU)

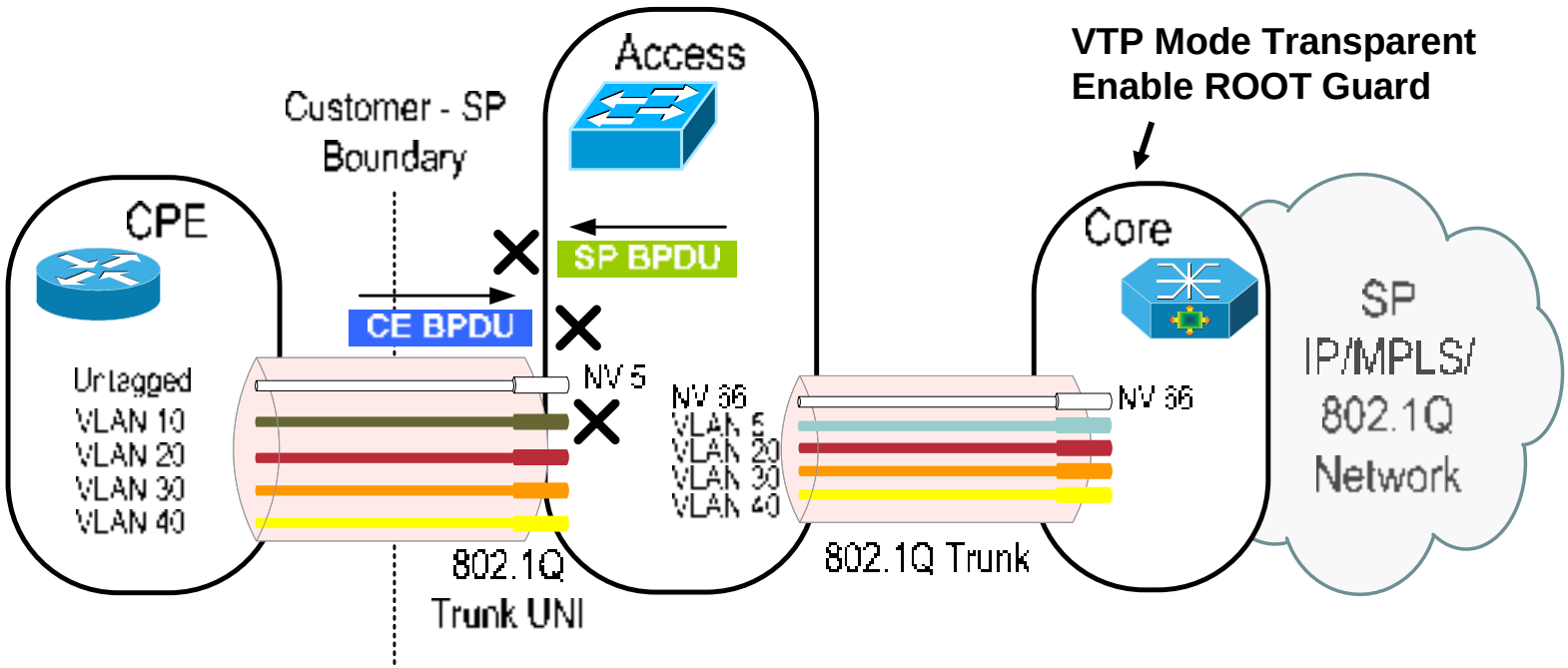


Enable Port Security
Enable 802.1X
Disable CDP
Remove VLAN 1 and Reserved VLANs from UNIs
Set DTP to "Non-Negotiate"
Prune All Unused VLANs from Allowed List
UNI VLANs Must Not Be Used as Native VLAN on SP Trunks

Ethernet Security: SP Recommendations



Ethernet Security: SP Recommendations

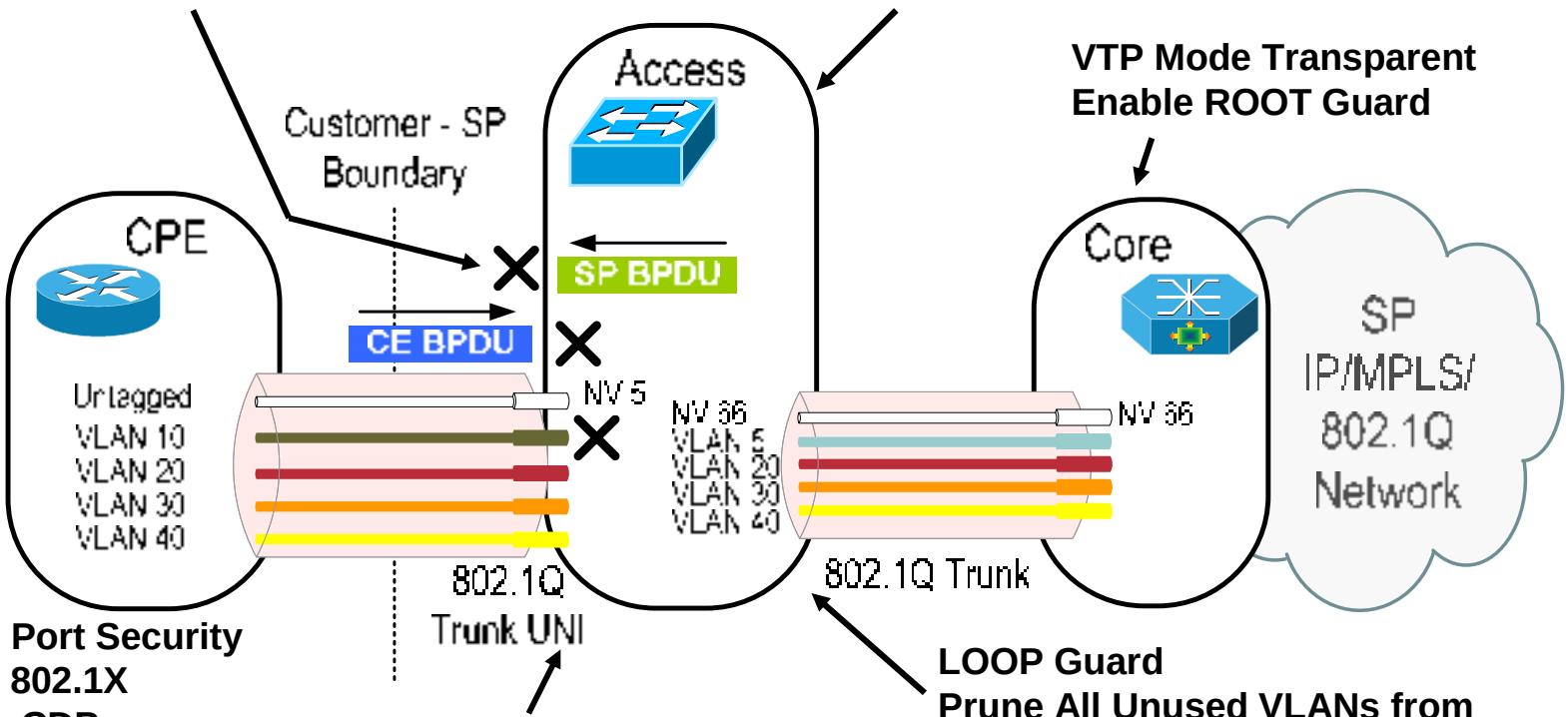


Ethernet Security: SP Recommendations

BPDU Filter (for Egress SP BPDU)
MAC ACLs (for Ingress CE BPDU)

Disable Password Recovery
VTP Mode Transparent

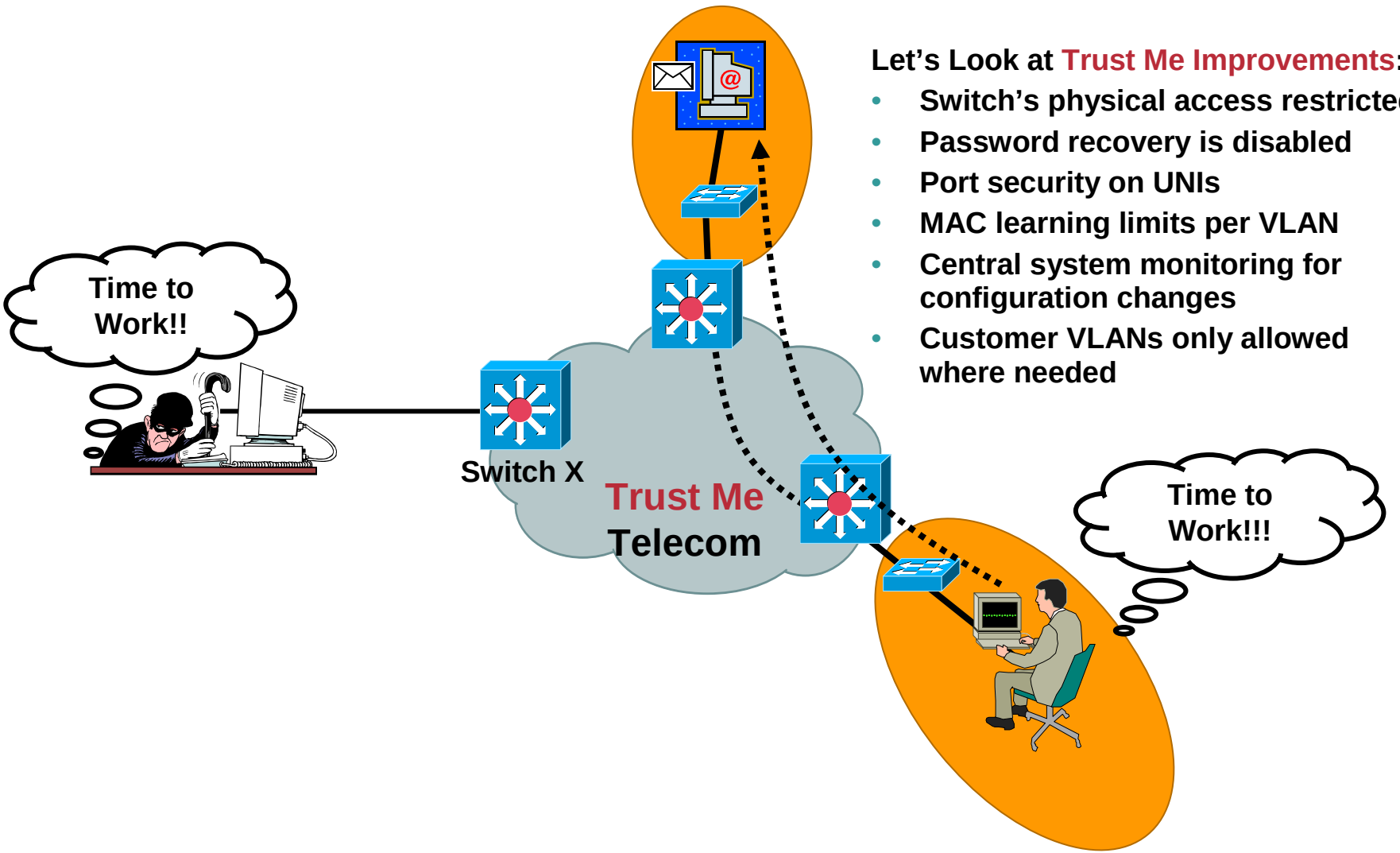
VTP Mode Transparent
Enable ROOT Guard



Enable Port Security
Enable 802.1X
Disable CDP
Remove VLAN 1 and Reserved VLANs from UNIs
Set DTP to "Non-Negotiate"
Prune All Unused VLANs from Allowed List
UNI VLANs Must Not Be Used as Native VLAN on SP Trunks

LOOP Guard
Prune All Unused VLANs from Allowed List
Remove VLAN 1 and Reserved VLANs from Trunks
Reserve a VLAN ID for the Native VLAN on the SP Trunks

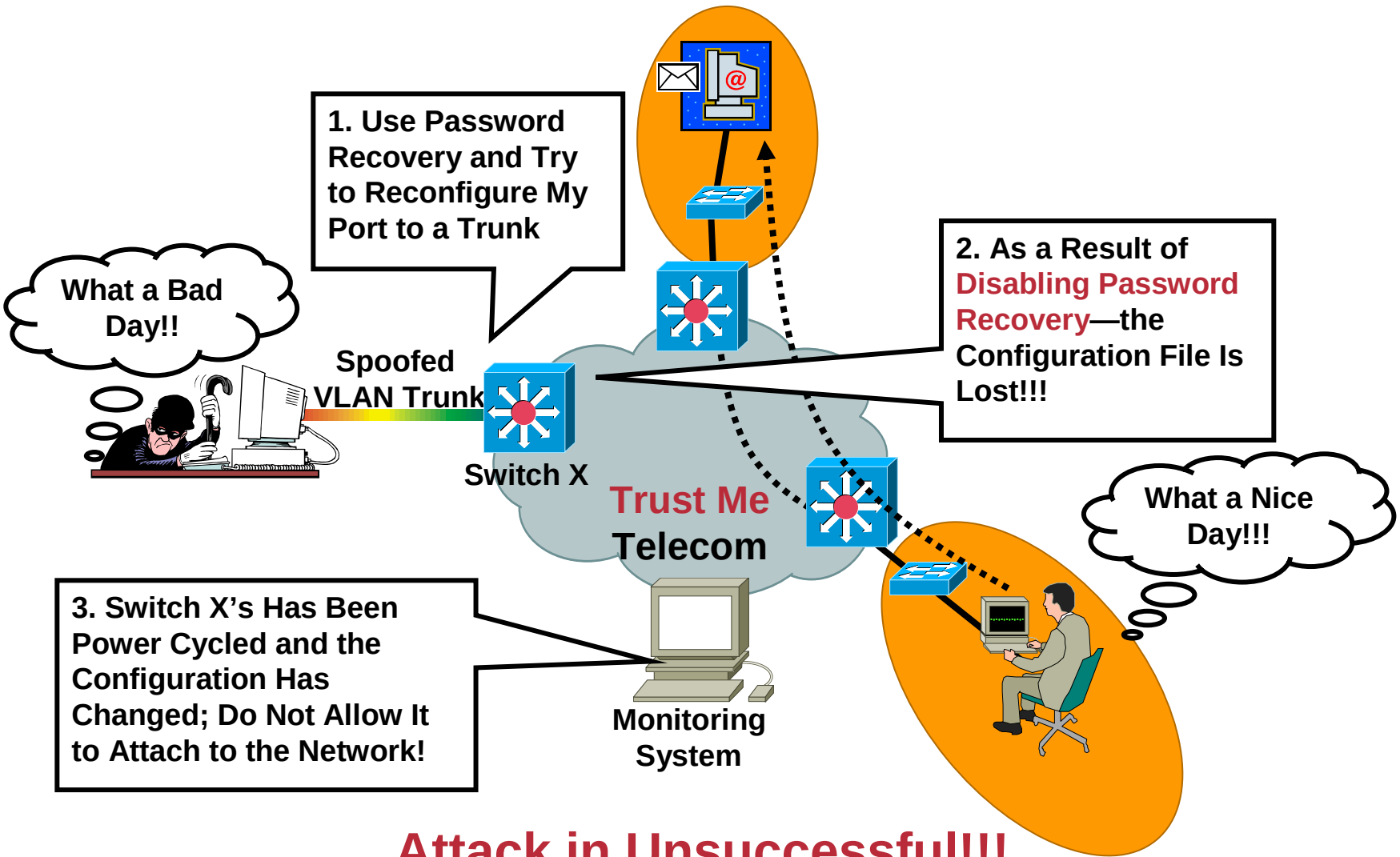
Ethernet Security: Proactive Security Management



Let's Look at Trust Me Improvements:

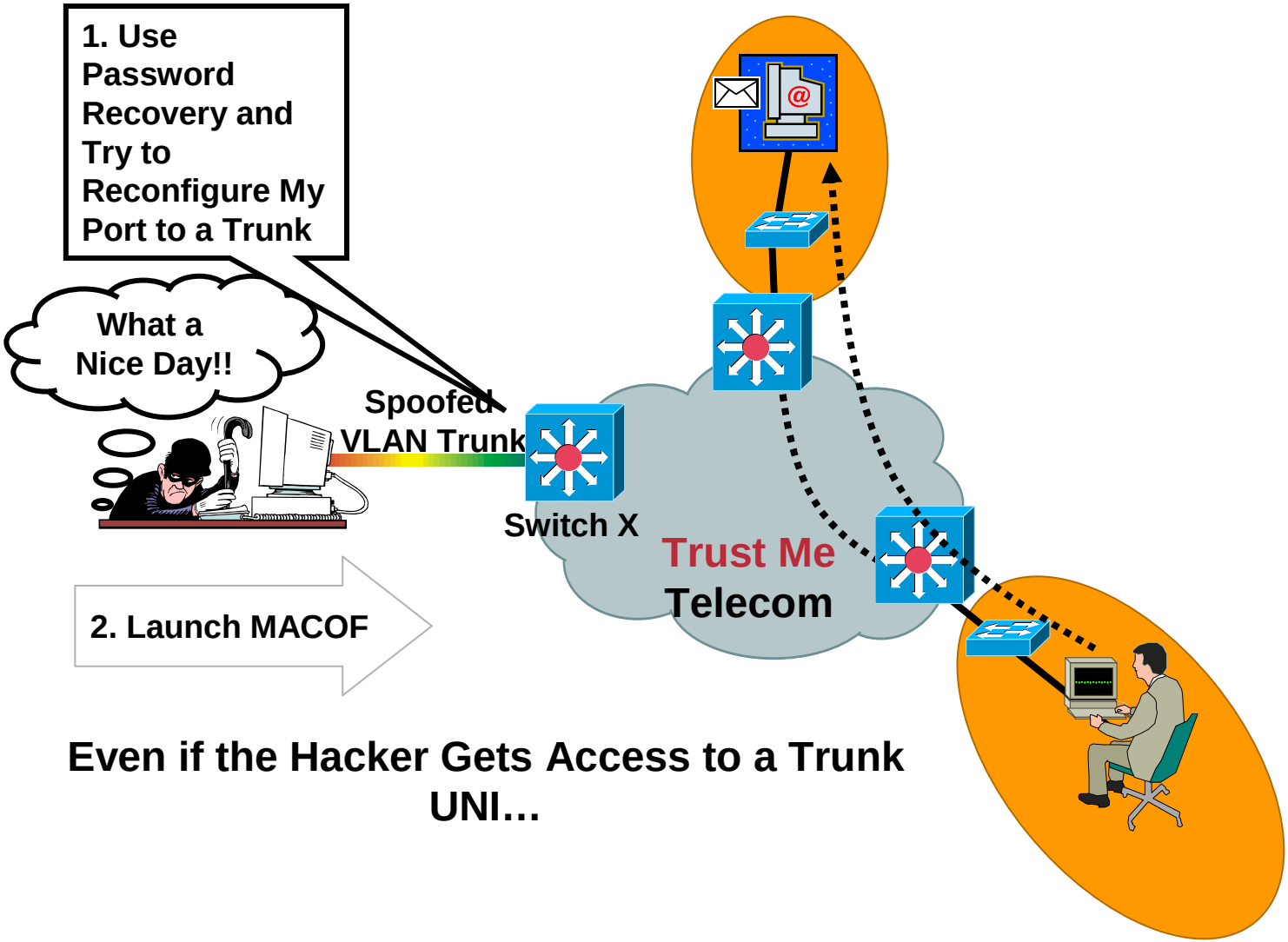
- Switch's physical access restricted
- Password recovery is disabled
- Port security on UNIs
- MAC learning limits per VLAN
- Central system monitoring for configuration changes
- Customer VLANs only allowed where needed

Ethernet Security: Proactive Security Management (scenario 1)



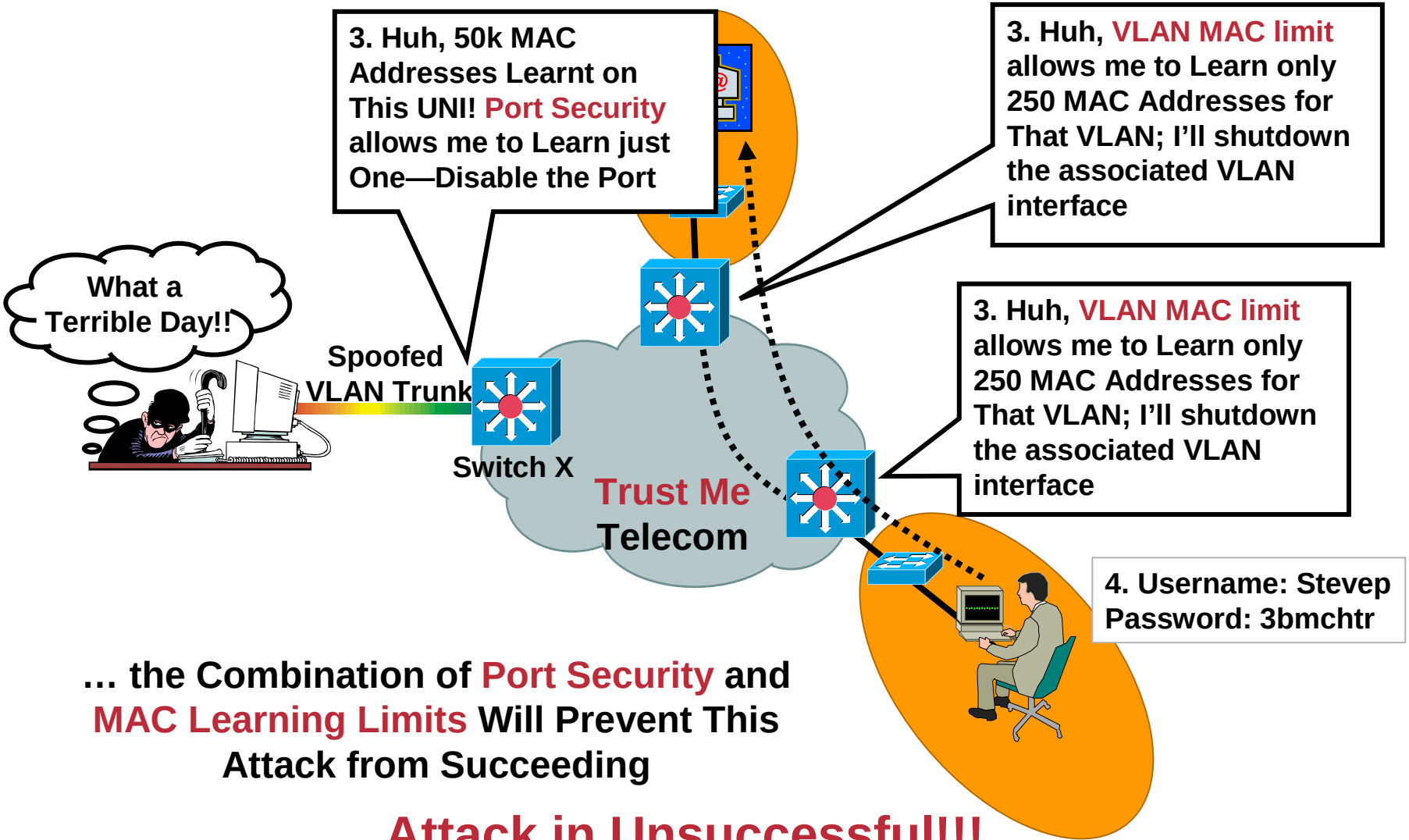
Attack in Unsuccessful!!!

Ethernet Security: Proactive Security Management (scenario 2)



Even if the Hacker Gets Access to a Trunk UNI…

Ethernet Security: Proactive Security Management (scenario 2)



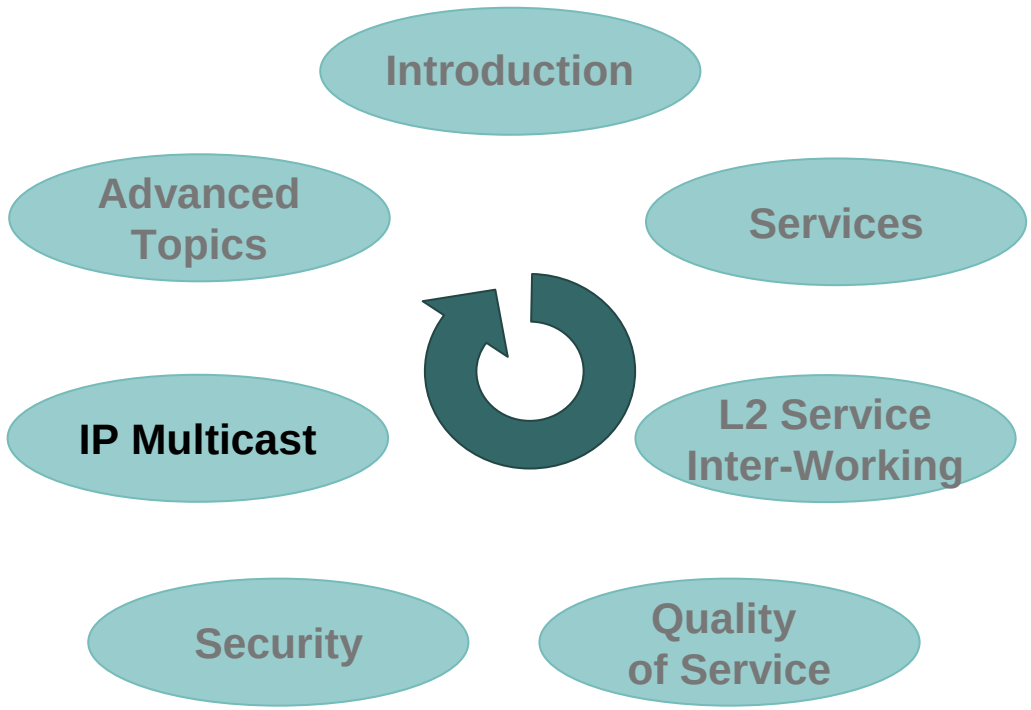
… the Combination of Port Security and MAC Learning Limits Will Prevent This Attack from Succeeding

Attack in Unsuccessful!!!

Ethernet Security—Summary

- **Be aware of the security risks**
  - **Whitepapers at http://naughty.monkey.org/~dugsong/dsniff/**
  - **Run dSniff against the service!**
- **Cisco has robust solutions today**
  - **RootGuard, Port Security, TACACs, etc.**
- **Cisco is working on several initiatives**
  - **802.1x supplicant**
  - **Anti-ARP spoofing mechanisms**
  - **MAC address limits per VLAN, and more…**
- **Please refer to http://www.cisco.com/go/safe**

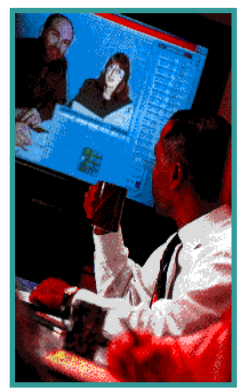
Agenda



Considerations for IP Multicast Traffic on a Metro Ethenet Network; How to Choose the Right Service for Multicast

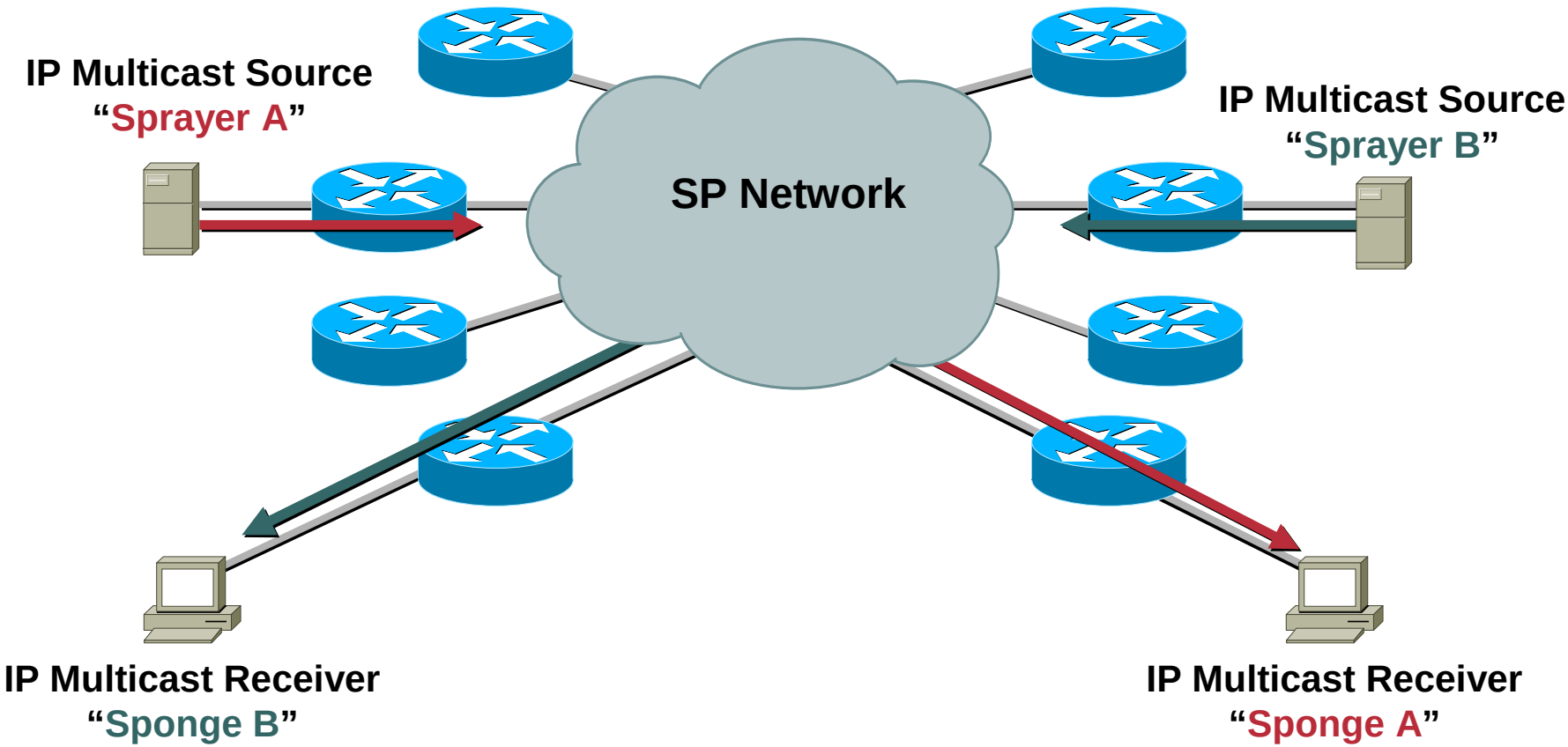
Why Is IP Multicast Important?

- IP Multicast used by one-to-many data push applications
- Data warehousing, finance applications
- IP Multicast enables the efficient delivery of data
- Considerable cost savings can be realized using IP Multicast for
  - Streaming media
  - Training and corporate communications
  - Video and audio conferencing



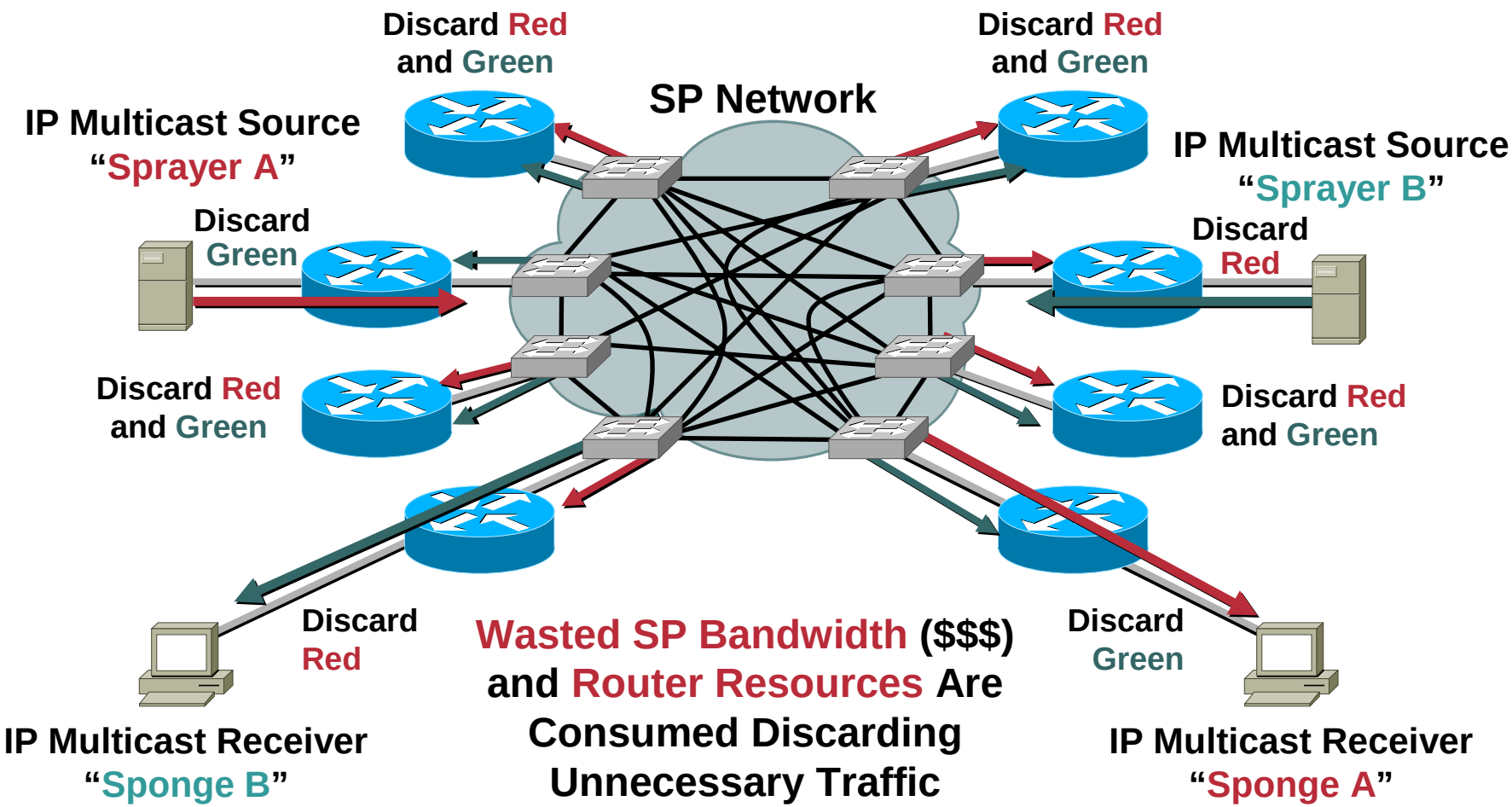
The Impact of IP Multicast on Metro Ethernet Services

This Is What We Expect of the SP for IP Multicast on a Multipoint service … constrained traffic

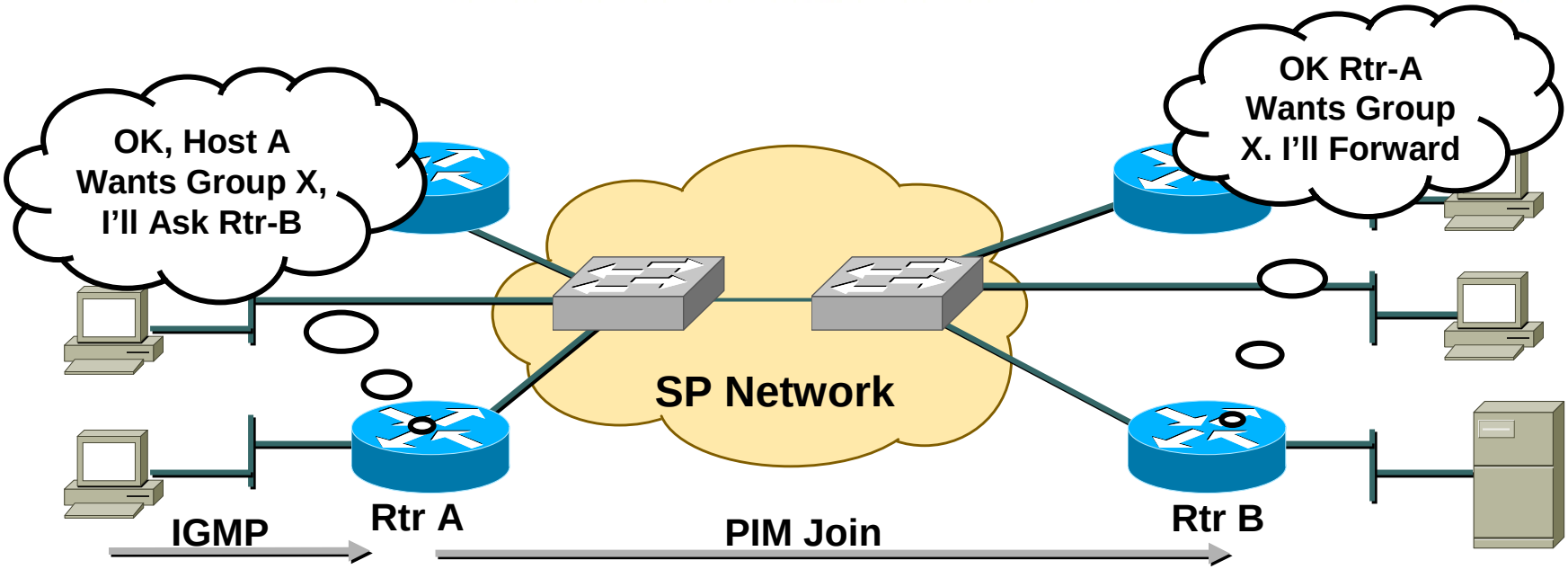


The Impact of IP Multicast on Metro Ethernet Services

And This Is What We might Get…



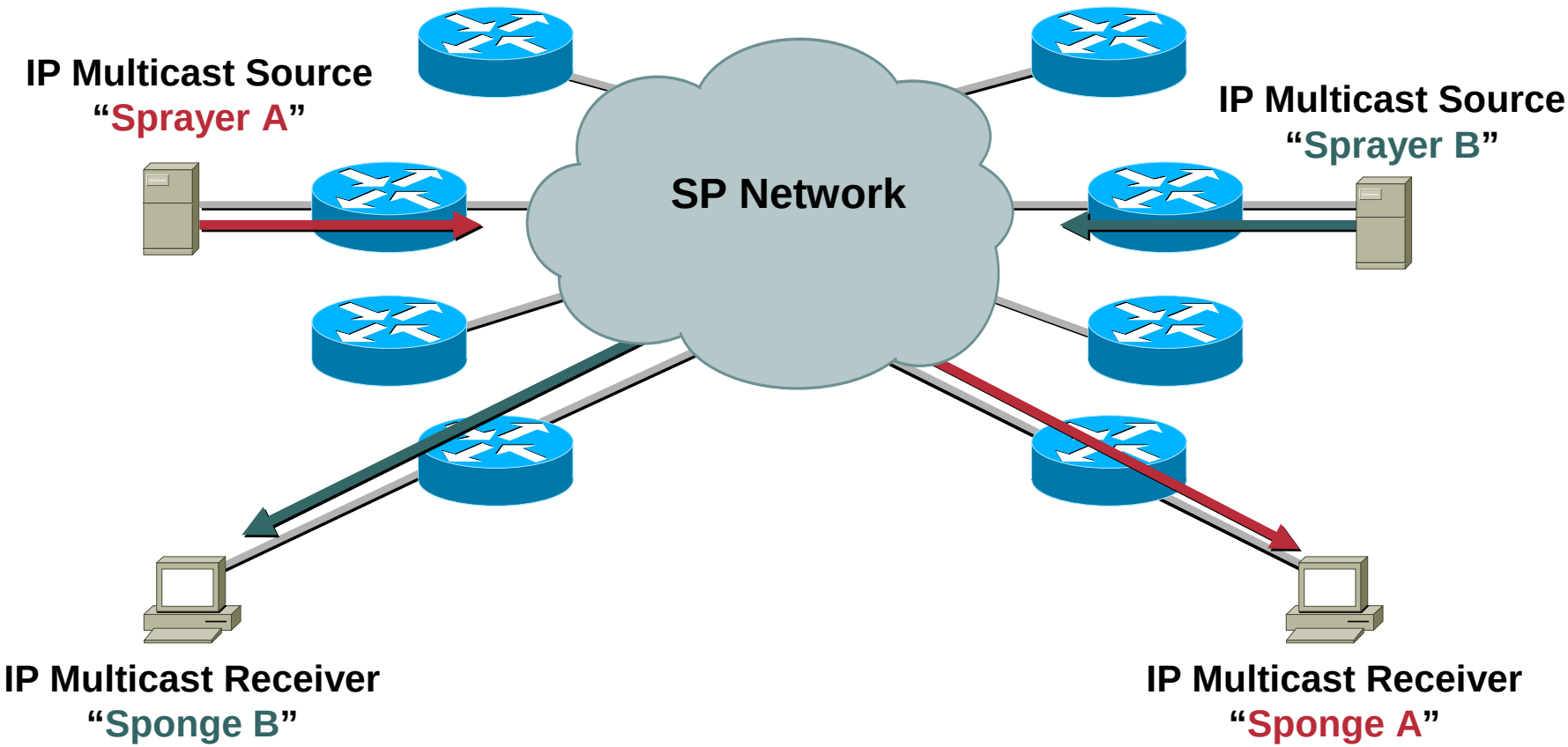
The Impact of IP Multicast on Metro Ethernet Services



- **SP Challenges with Multicast on Multipoint services**
  - **Constrain Multicast traffic at Layer 2**
  - **802.1Q Tunnelling and its effect on snooping features**
  - **RGMP / IGMP snooping / PIM snooping**

The Impact of IP Multicast on Metro Ethernet Services

This Is What We Expect of the SP for IP Multicast on a Point to Point service …



The Impact of IP Multicast on Metro Ethernet Services

This Is What We get for IP Multicast on an Point to Point service …

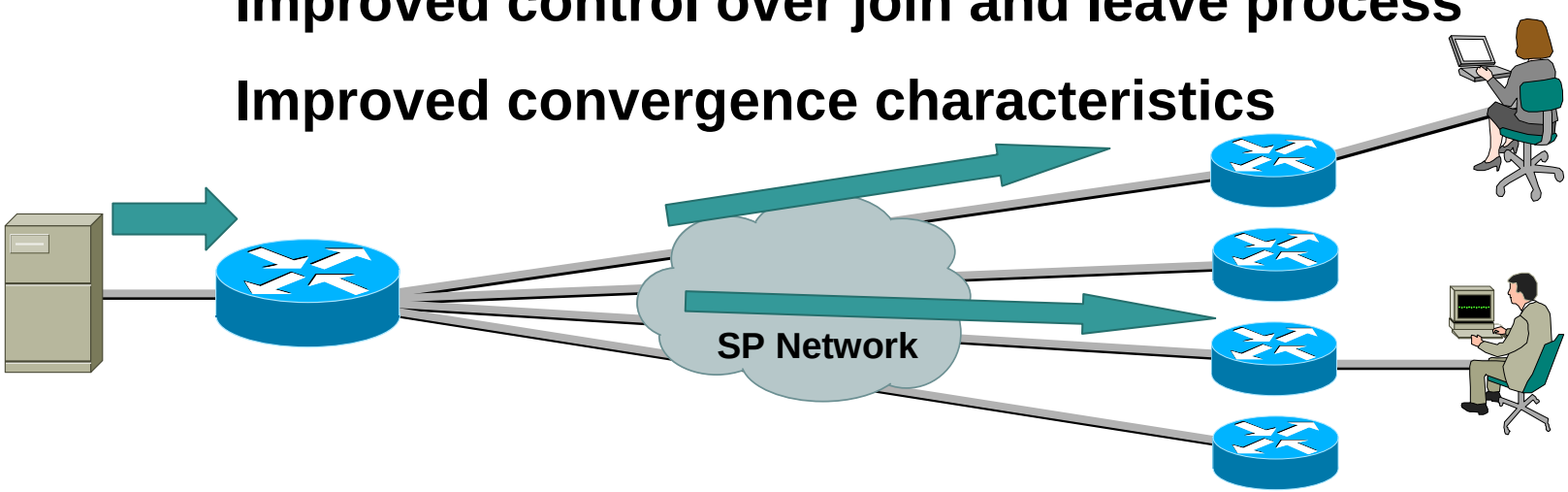
- **IP multicast constrained to those sites that actually request the data**

Enterprise has complete control

Reduced resource and bandwidth overhead

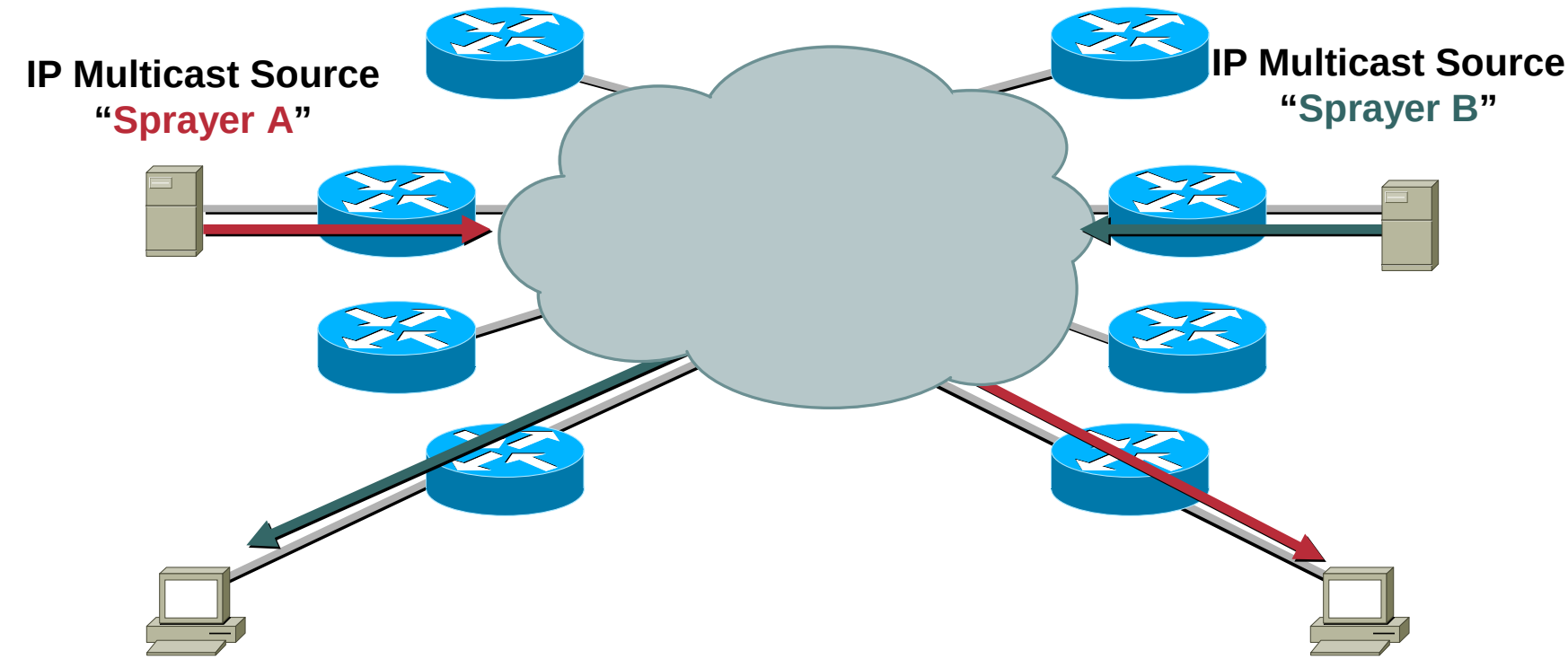
Improved control over join and leave process

Improved convergence characteristics



L3VPN: The Impact of IP Multicast

This Is What We Expect…and Get!!!



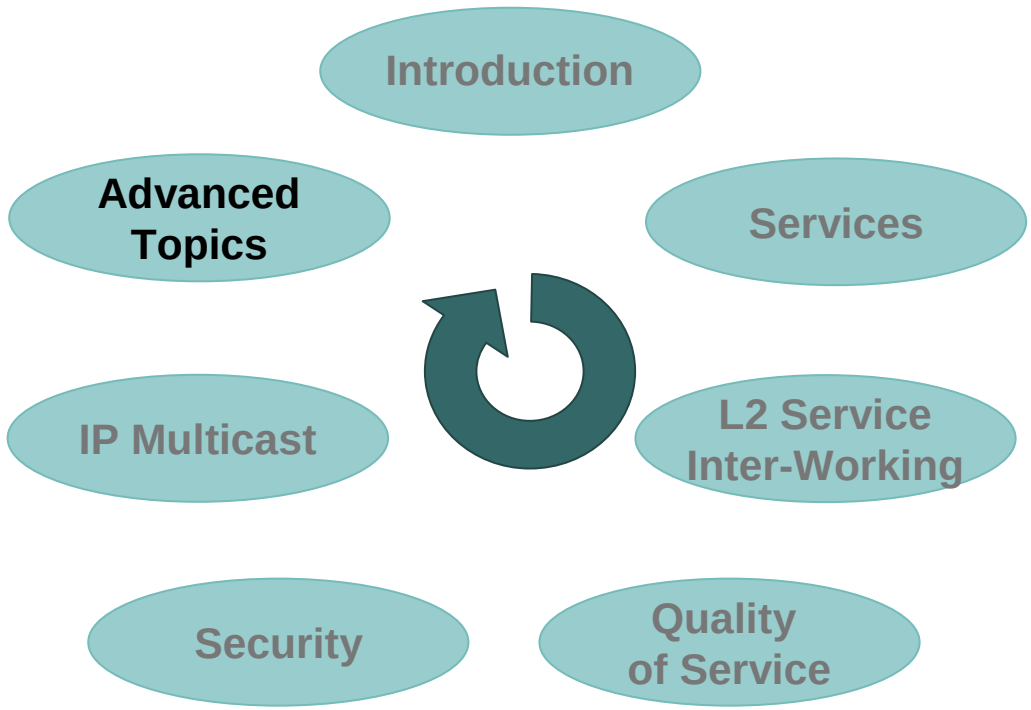
Metro Ethernet - IP Multicast considerations

- **IP Multicast should be considered when selecting Metro Ethernet services**
- **If an Enterprise has…**
  - **A large volume of IP Multicast traffic**
  - **Mismatched bandwidth i.e. 10/100/1000 connected sites**
  - **… A MultiPoint service may be a poor service choice**
- **Point to Point Metro Ethernet services or Layer 3 Multicast enabled VPN are better solutions for IP Multicast**
- **The Service Provider must also consider IP Multicast replication as it will consume system resources and bandwidth**

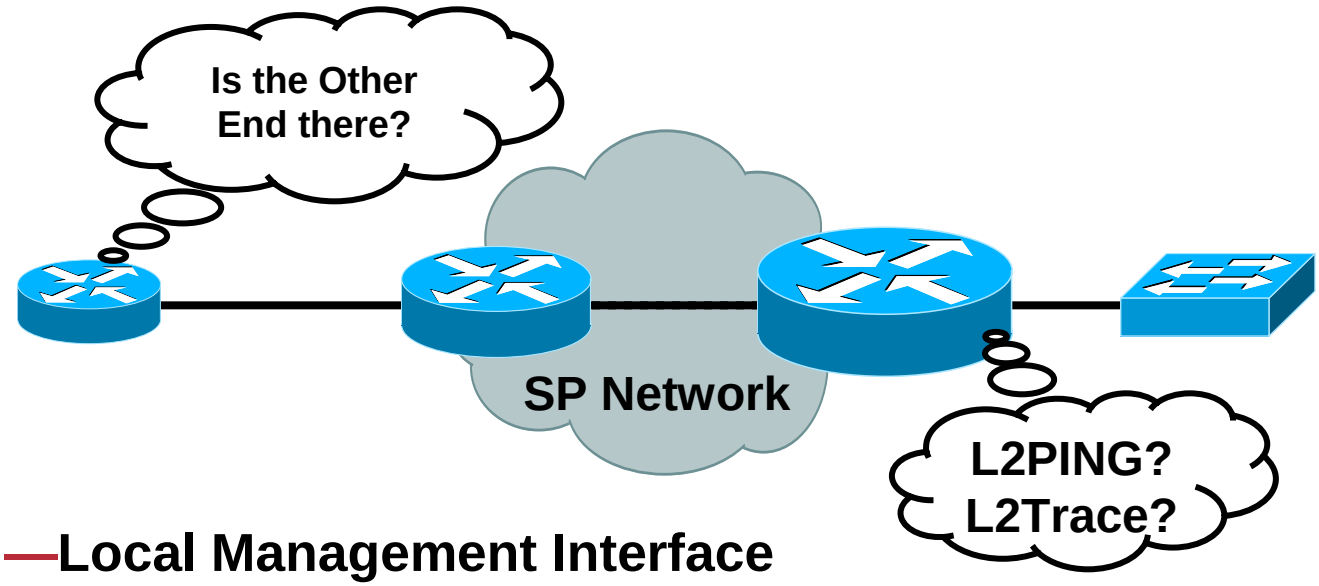
Agenda

Cisco.com

Evolution of Ethernet with Support for LMI and OAM Signaling; What Standards Bodies Are Involved



Ethernet LMI and End-to-End OAM



- LMI—Local Management Interface
- OAM—Operation, Administration and Maintenance
- Ethernet services offer very flexible and high-speed service offerings at Layer 2 and Layer 3, but…
- Ethernet lacks certain "carrier class" features such as LMI and OAM functions
- Several industry bodies are investigating functions that are available in Layer 3

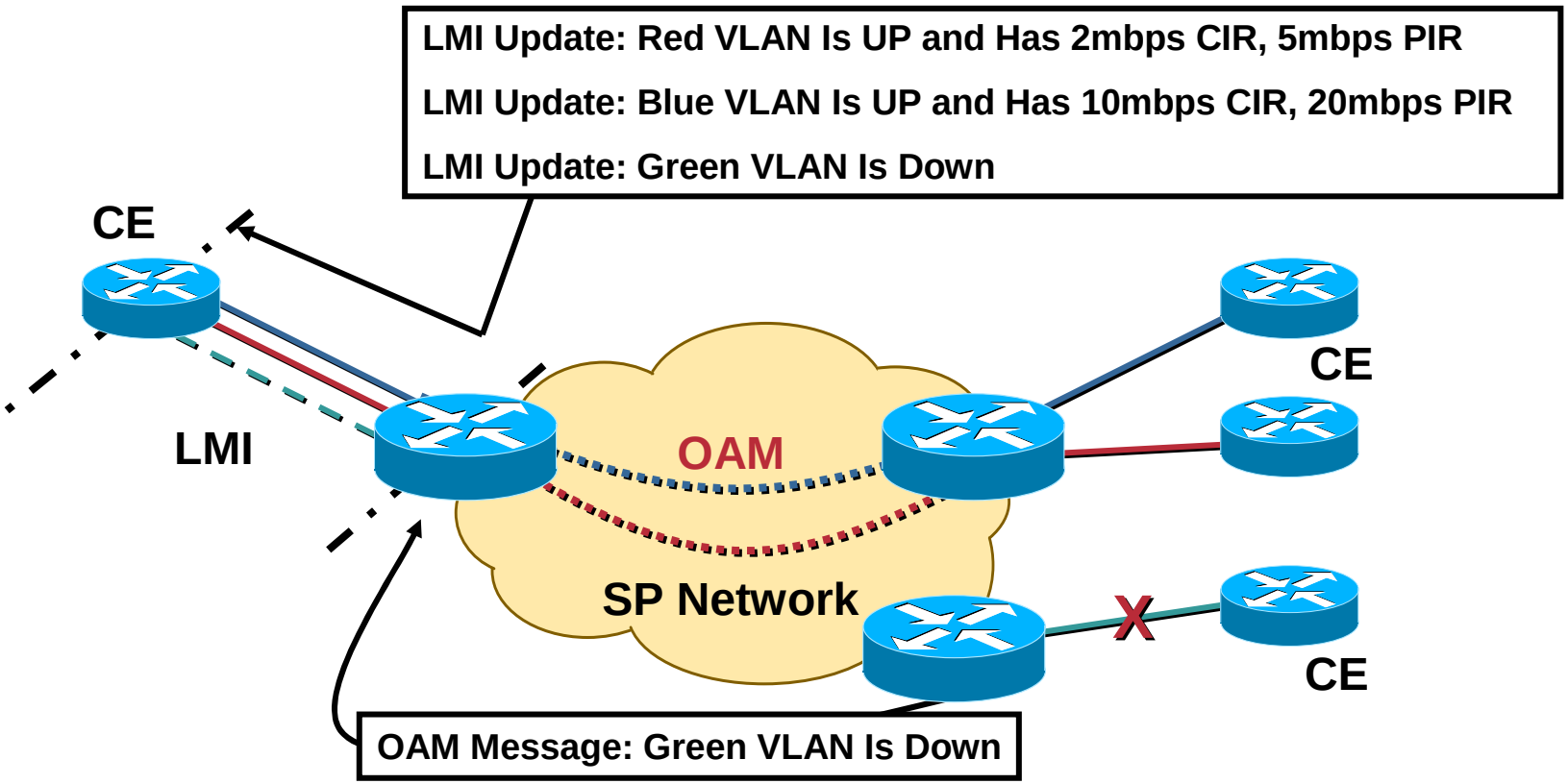
Ethernet Local Management Interface (LMI)

- An LMI informs a CPE device about the state of the interconnecting circuit and can signal other information such as bandwidth parameters, network addresses, etc
- Relevant to point-to-point circuits such as ATM PVCs, Frame Relay DLCIs and now being looked at for Ethernet
- ERS/EWS models Frame Relay or ATM using VLAN IDs as VC identifiers

  Ethernet LMI will be an important development for Ethernet service adoption

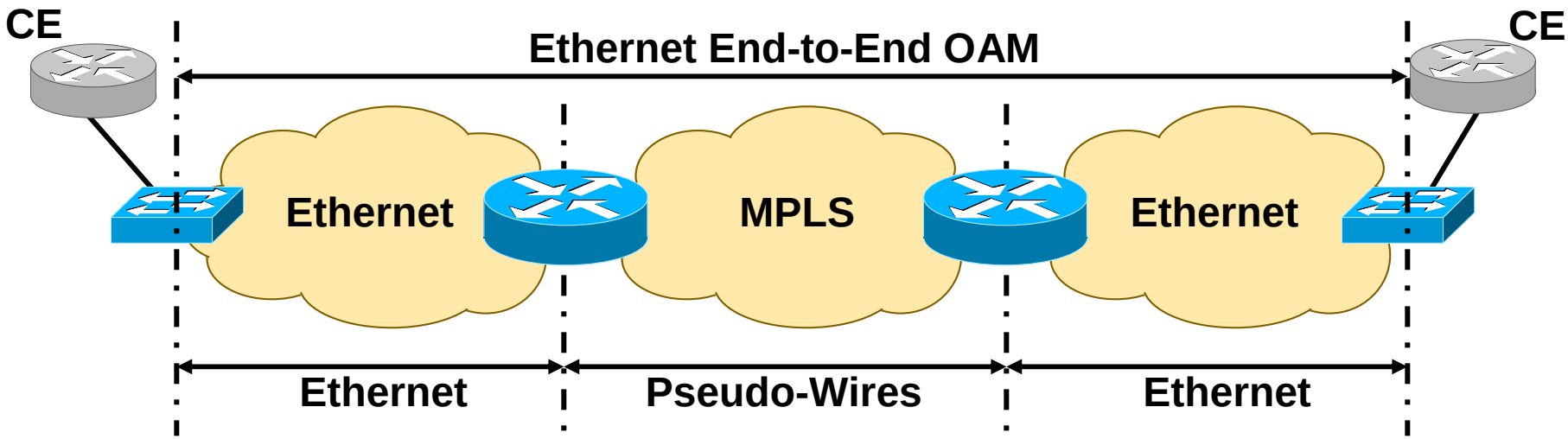
- Not a trivial issue to resolve due to architectural considerations
- Also requires and end-to-end signaling mechanism to carry far end circuit state (OAM)

Ethernet LMI Operation



- OAM end-to-end signaling of connection state
- LMI signals end-to-end state to customer devices

End-to-End Ethernet OAM

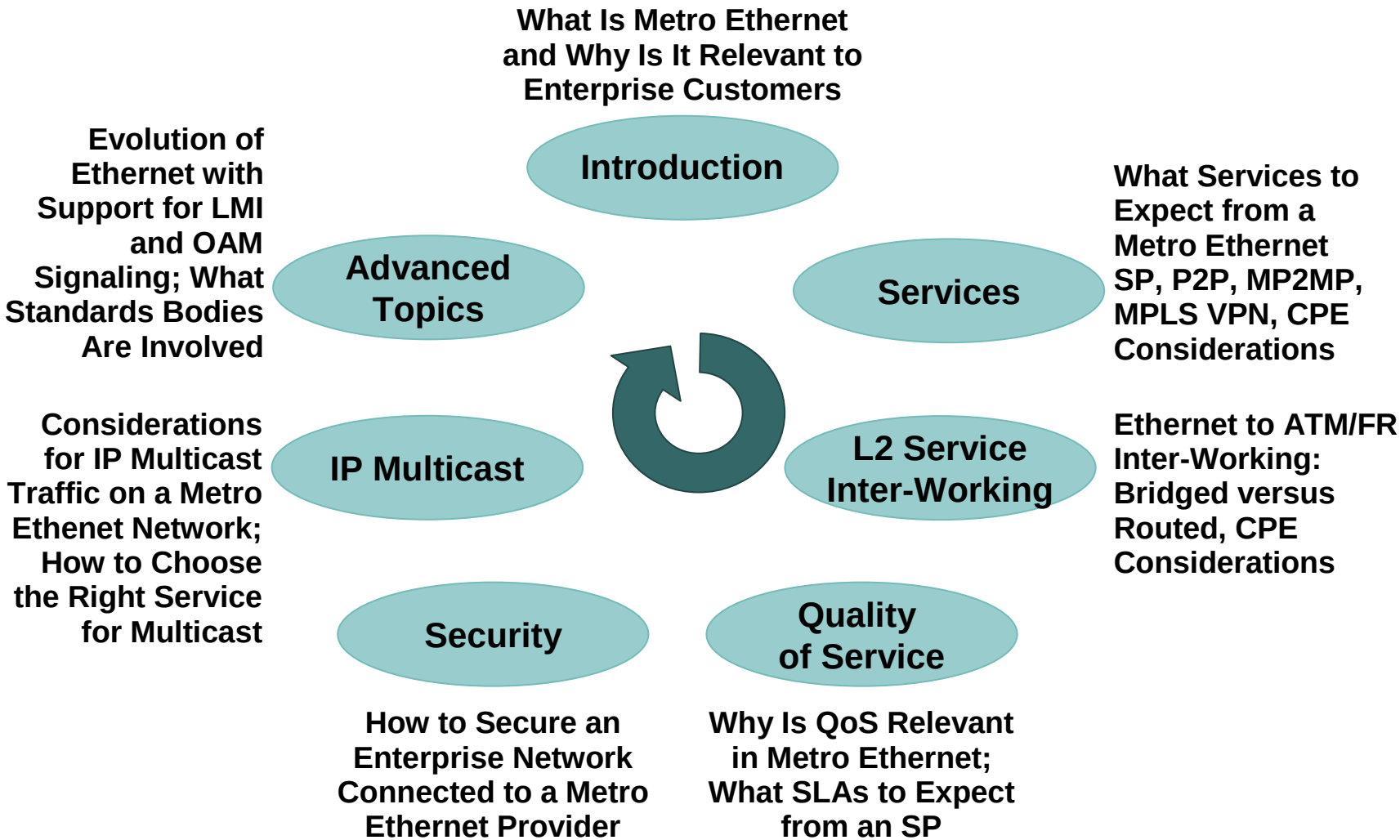


- End-to-End OAM is complex due to different (or non-existents) signaling mechanisms
- Service inter-working further complicates the problem
- Protocol layering also plays a part

End-to-End Ethernet OAM

- Ethernet OAM and LMI will be a significant enabler of Ethernet services and will speed adoption
- Early drafts being produced now, but is a very complex area
- Metro Ethernet Forum (MEF) and IEEE investigating Ethernet OAM and LMI
  - L2PING and Trace for MAC addresses
  - Ethernet LMI and OAM interaction across different protocol boundaries
  - OAM Inter-Working (ATM to Ethernet)
- ITU-T and IETF also investigating OAM but generally with respect to specific transport requirements
- Cisco is active within IEEE, MEF, IETF and ITU-T in driving solutions and standards for Ethernet OAM and LMI functions

Agenda



Unified VPN Platform Solutions