Virtual Private Networks

Design of Telecommunication Infrastructures
2008-2009

Rafael Sebastian
Departament de tecnologies de la Informació i les Comunicaciones
Universitat Pompeu Fabra

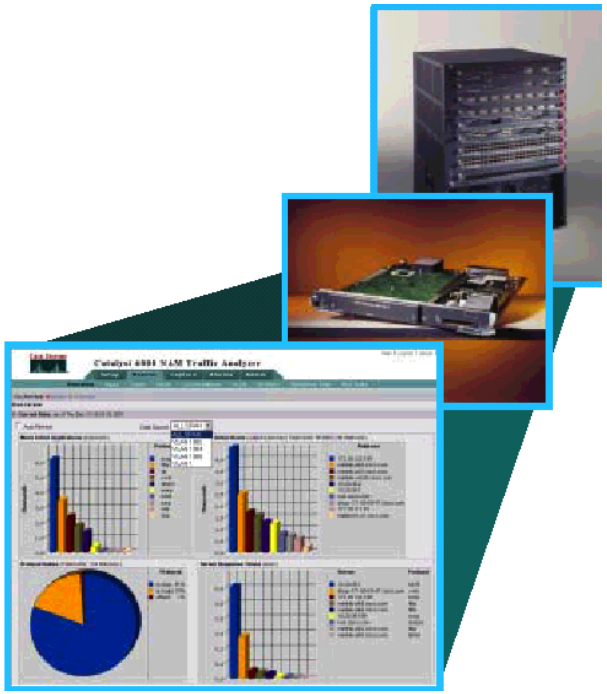
Goals of the section

- ☑ Differentiate between VPN types
- ☑ Differences between overlay VPN and peer-to-peer VPN
- ☑ Major technologies supporting overlay and peer-to-peer VPNs

Table of Contents

- **Overlay VPNs**
- Peer-to-peer VPNs
- Overlay vs P2P VPNs

- Review Questions



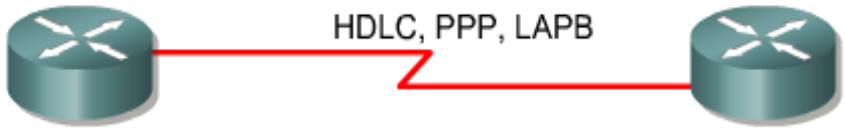
Overlay VPNs

- Point-to-Point Connections
- Virtual Private Networks
- VPN Routing
- Tunneling Protocols

Point-to-Point Connections

- Point-to-Point connection or *leased lines* are not VPNs
- Guaranteed bandwidth and privacy through the service
- They are more expensive (no statistical multiplexing)
- Customers are fully unaware of the infrastructure behind

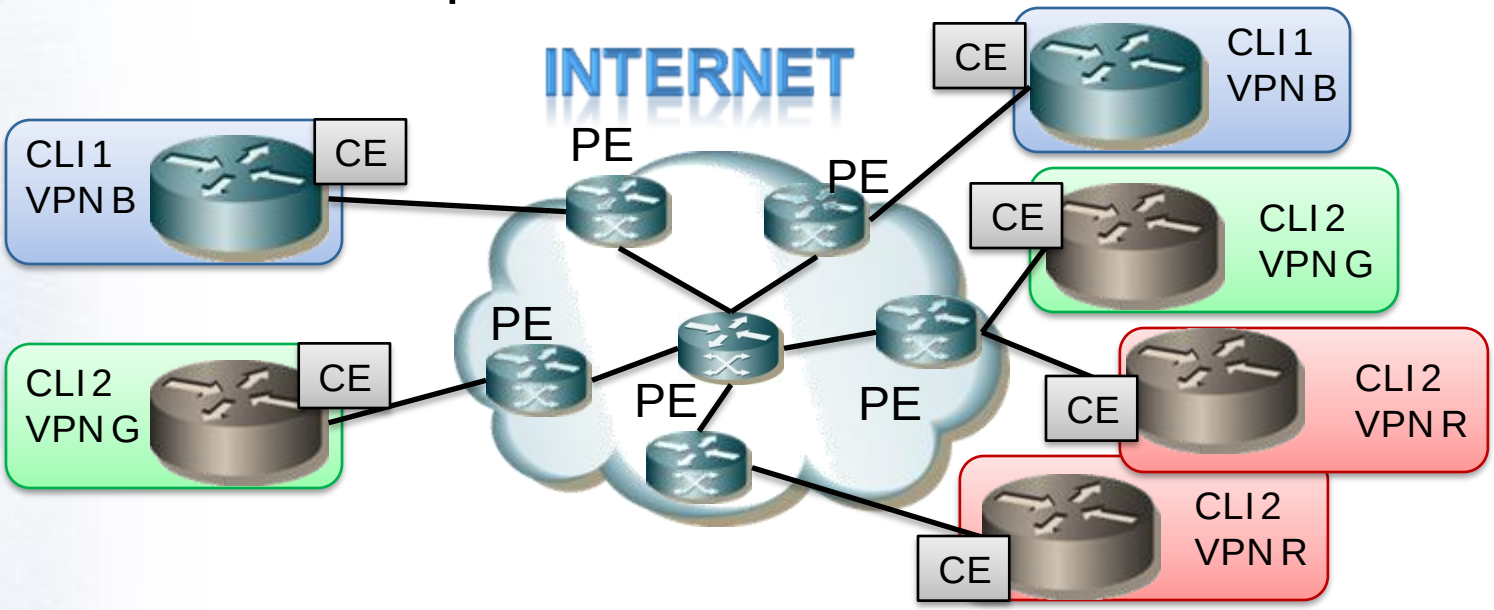
Dedicated lines



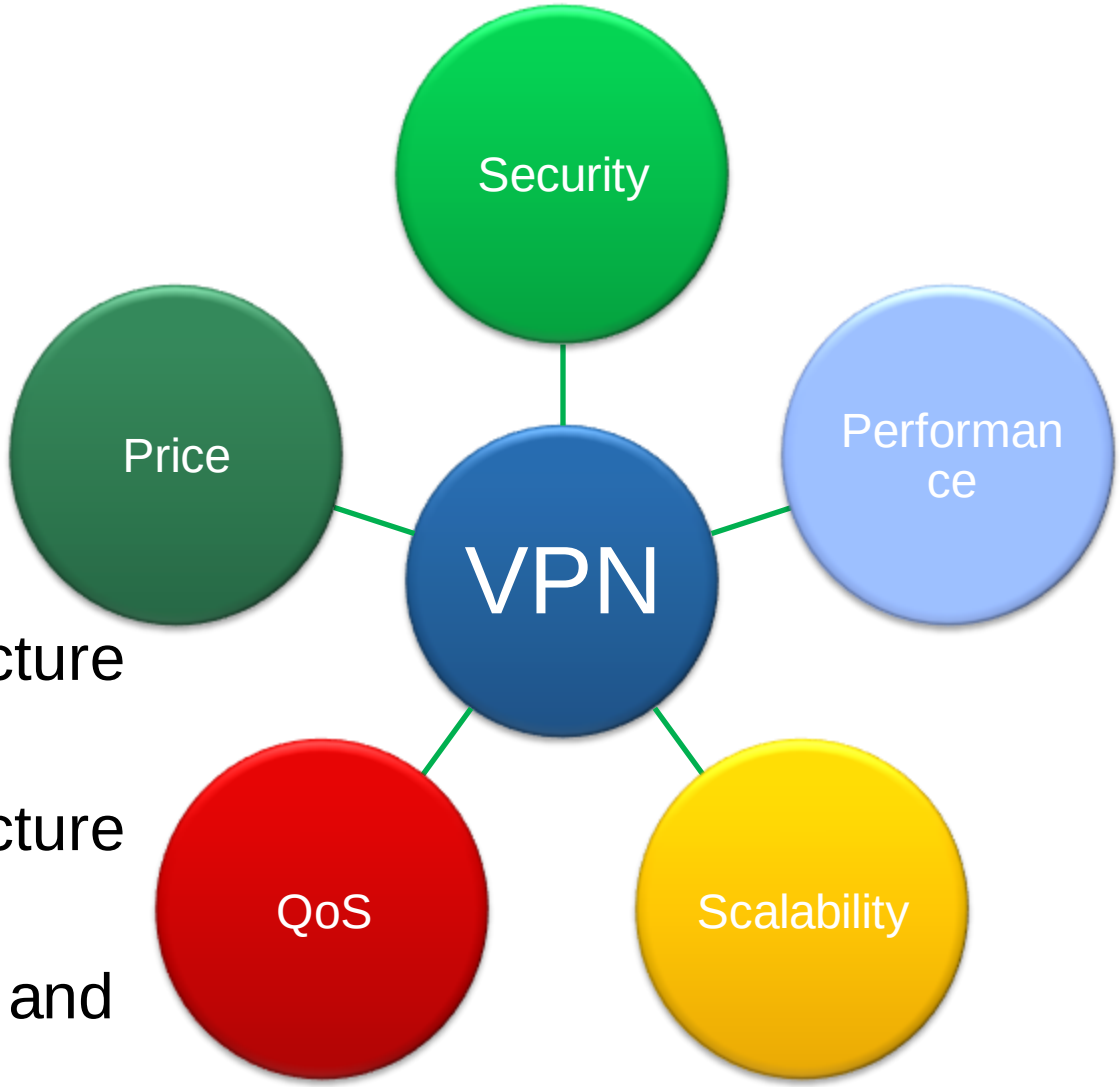
Packet switching

Virtual Private Networks

- Alternative to point-to-point connections
  - same benefits
  - less cost
- Uses a public shared infrastructure but with the benefits of a private network



Virtual Private Networks



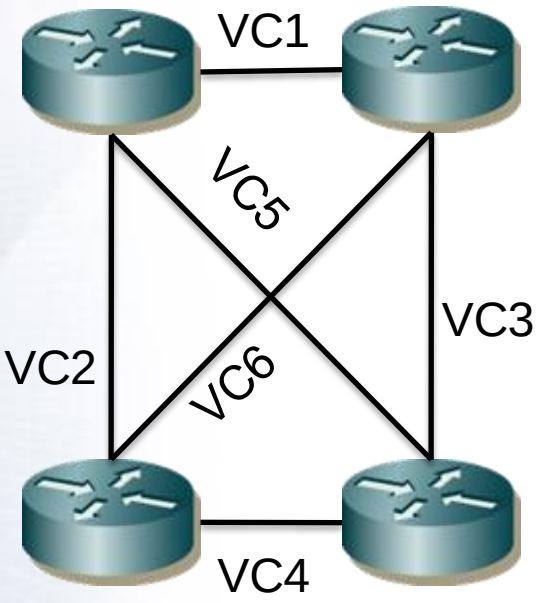
- Share the infrastructure with other users
- Share the infrastructure for other services
- Simpler to manage and maintain

Classification of VPNs

- **Depending on the termination**
  - Overlay VPN (Based on CE)
  - Peer-to-peer VPN (Based on PE)
- **OSI Layer Level**
  - VPN Layer 2
  - VPN Layer 3
- **Service provider technology network**
  - IP, IP/MPLS, ATM, Frame Relay, SONET/SDH, X.25
- **Tunnel technology used**
  - IPSec, L2TP, PPTP, MPLS-LSP, ATM-VP/VC, Frame Relay VC, PPP/Dial-up
- **Topology of the network**
  - Full-Mesh, Partial Mesh, Hub-and-spoke

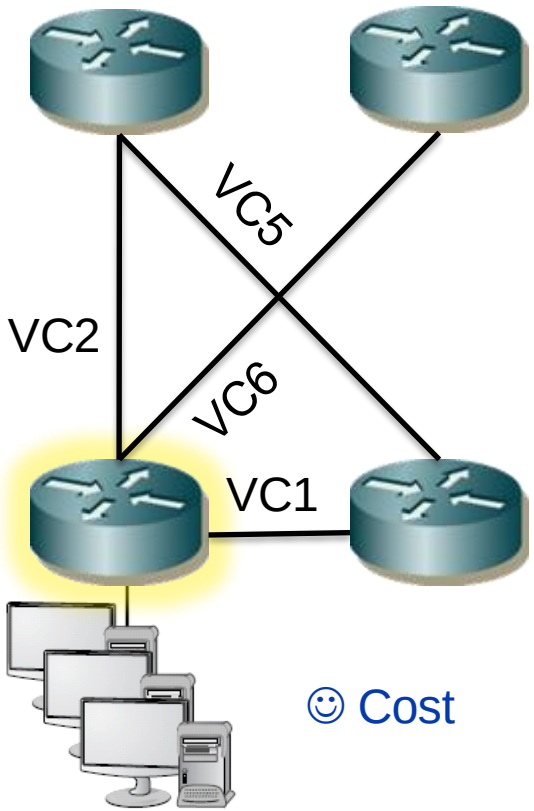
Network Topologies

Full-Mesh



☺ Optimal routing
☺ Redundancy
☹ Scalability
☹ Cost

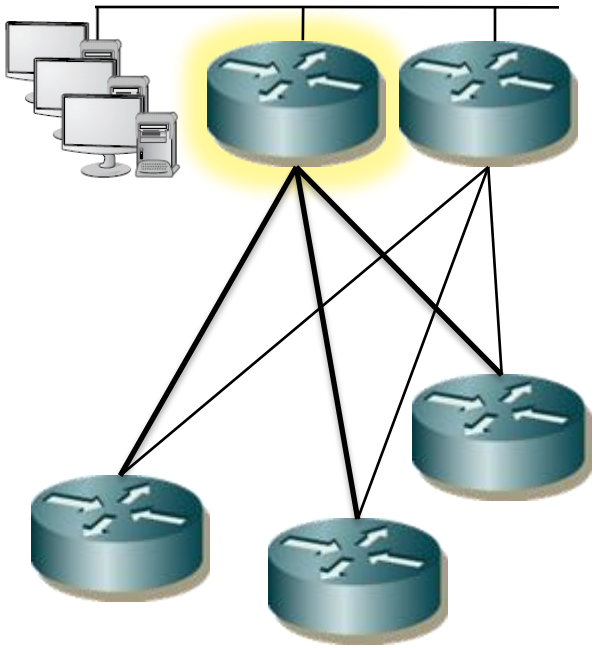
Partial-Mesh



☺ Cost

Redundant

Hub-and-Spoke



☺ Cost
☹ Redundancy

Which topology should I use?

- Topology dictated by business problem
- Overall categories:
  - Topologies influenced by the overlay VPN model
    - Logical and VC dependent topologies
  - Extranet topologies, any-to-any vs. central services
    - Topology as a function of security requirements
  - Special purpose topologies, VPDN

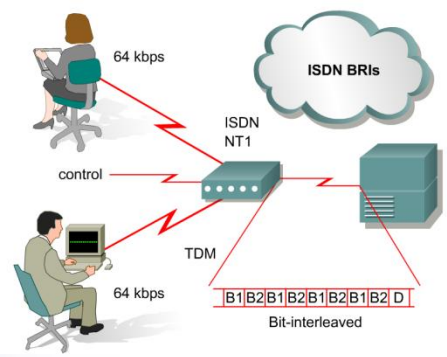
VPN Technologies – L1

Layer 1

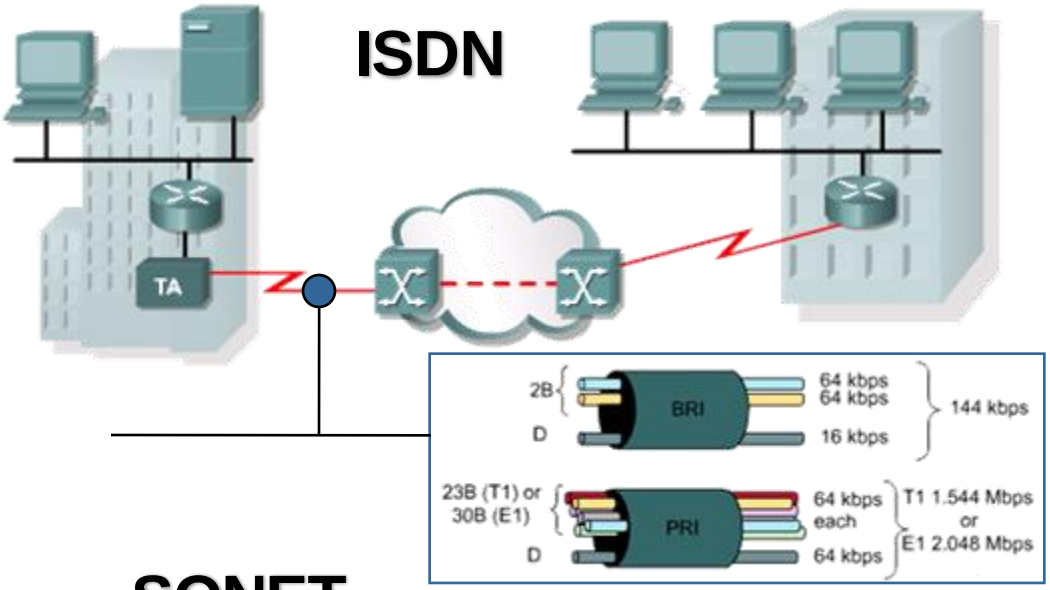
Physical layer VPNs

(SONET, E1/T1, ISDN)

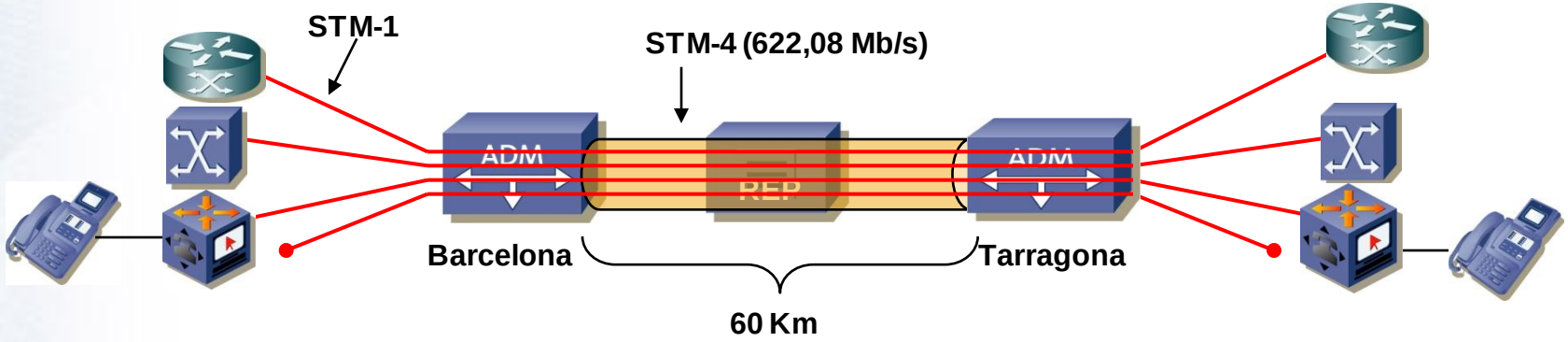
Connection Oriented



ISDN



SONET



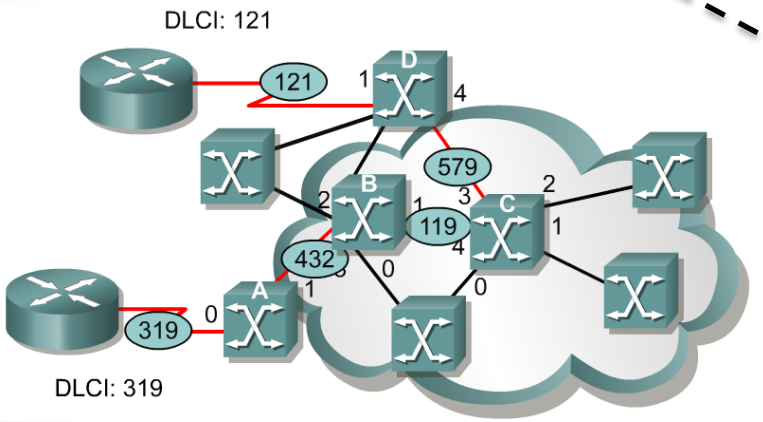
VPN Technologies – L2

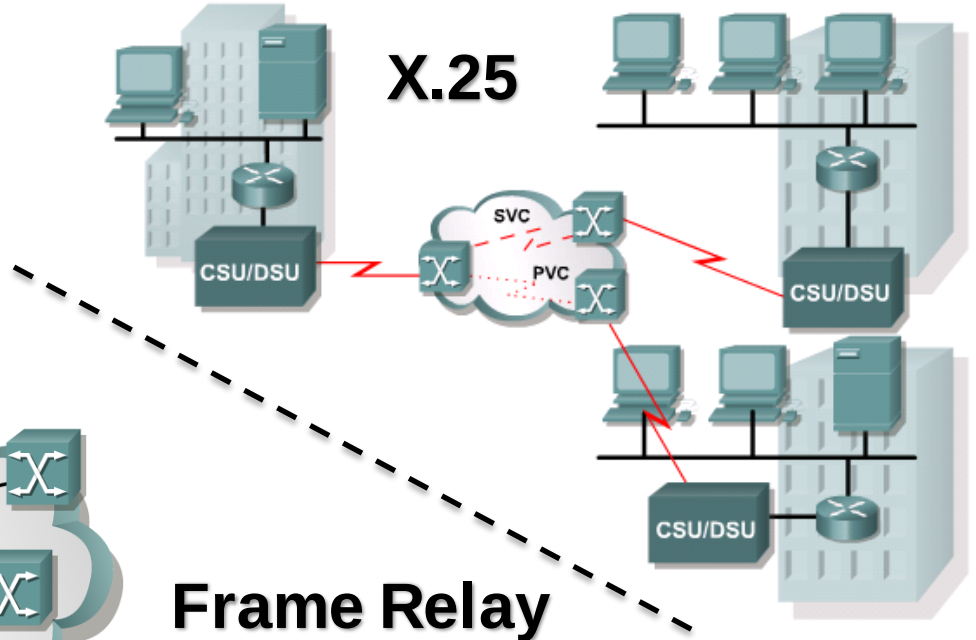
Layer 2

Link layer VPNs

(Frame Relay, X.25, ATM**)**

Connection Oriented





A				B				C				D			
VC	Port	VC	Port	VC	Port	VC	Port	VC	Port	VC	Port	VC	Port	VC	Port
319	0	432	1	432	3	119	1	119	4	579	3	579	0	121	1

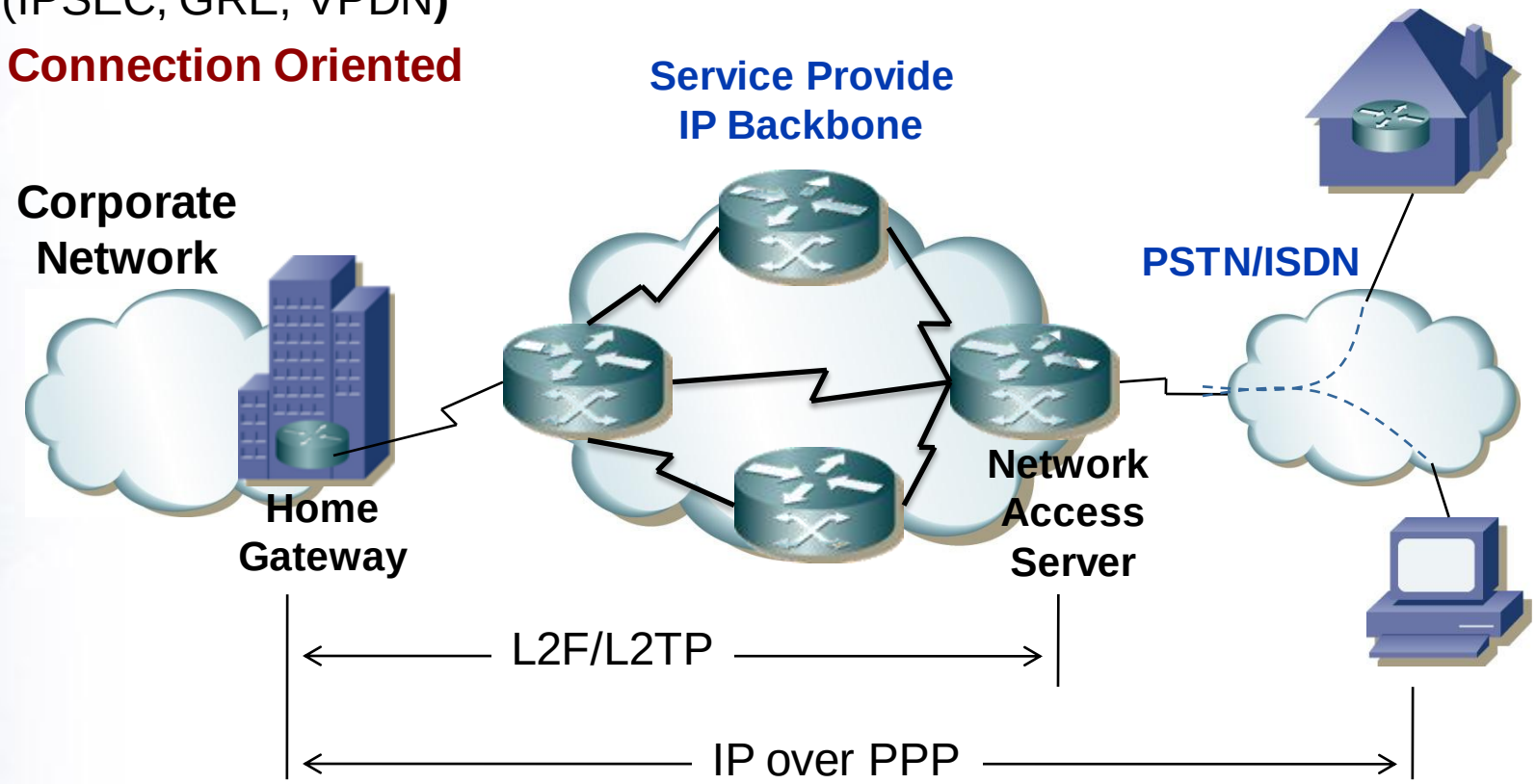
VPN Technologies – L3

Layer 3

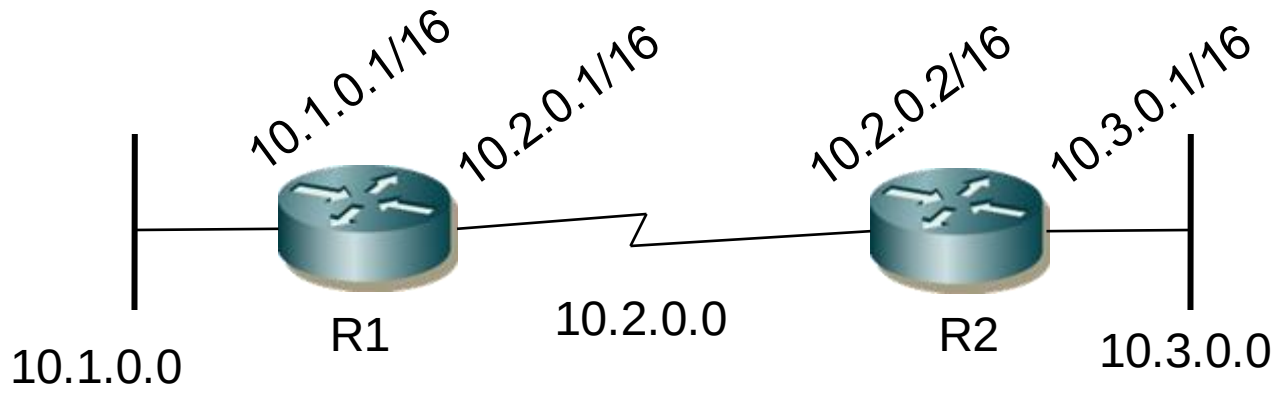
Network layer VPNs

(IPSEC, GRE, VPDN**)**

Connection Oriented



VPN Routing -
Point-to-point network



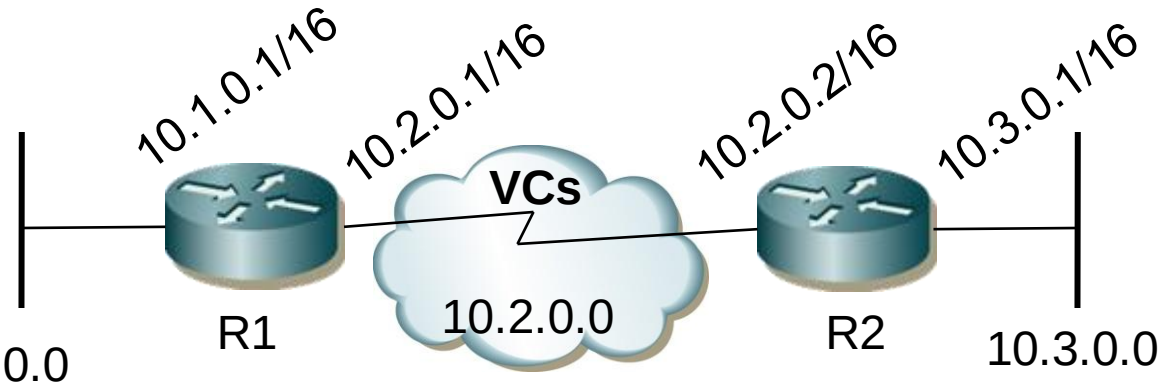
R1

Network	Method	Interface
10.1.0.0	Directly connected	Ethernet0
10.2.0.0	Directly connected Serial 0	Serial 0

R2

Network	Method	Interface
10.3.0.0	Directly connected	Ethernet0
10.2.0.0	Directly connected Serial 0	Serial 0

VPN network



R1

Network	Method	Interface
10.1.0.0	Directly connected	Ethernet0
10.2.0.0	Directly connected	Serial 0
10.3.0.0	RIP	Serial 0

R2

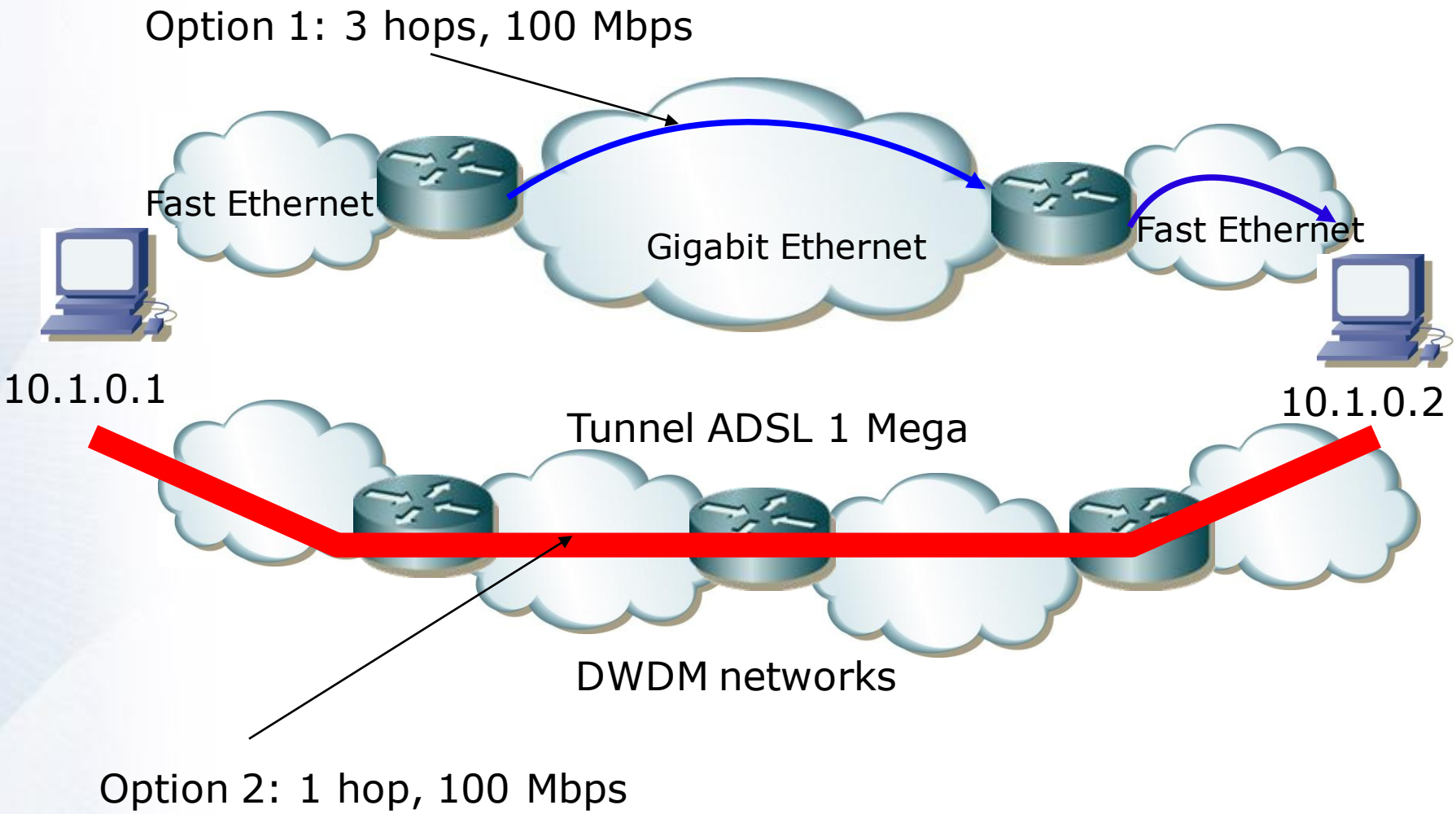
Network	Method	Interface
10.1.0.0	RIP	Serial 0
10.2.0.0	Directly connected	Serial 0
10.3.0.0	Directly connected	Ethernet0

There is no service provider infrastructure showing up on the customer routers R1 and R2!!
R1 and R2 are on a private and isolated connection

Tunnel Issues

- High-Level knowledge of public network security
- Tunneling is resource-intensive
  - Packet handling = CPU power
- Tunnels look “short”, but they aren't!
  - Beware of false routing decisions!
  - And routing loops
    - e.g. For IP-in-IP
- Check your Max. MTU before tunneling

Unexpected Routing Paths



Tunnels & routing

- Problem: Routing decisions are orthogonal to tunneling!
  - Routing loops: You take the routing decision twice!
  - Shortest path: “shortest” is not always best!
- Solution: Fool the routing algorithm
  - Give unattractive metrics to tunnels
  - Prevent duplicate routing
  - ...or simply use more intelligent protocols

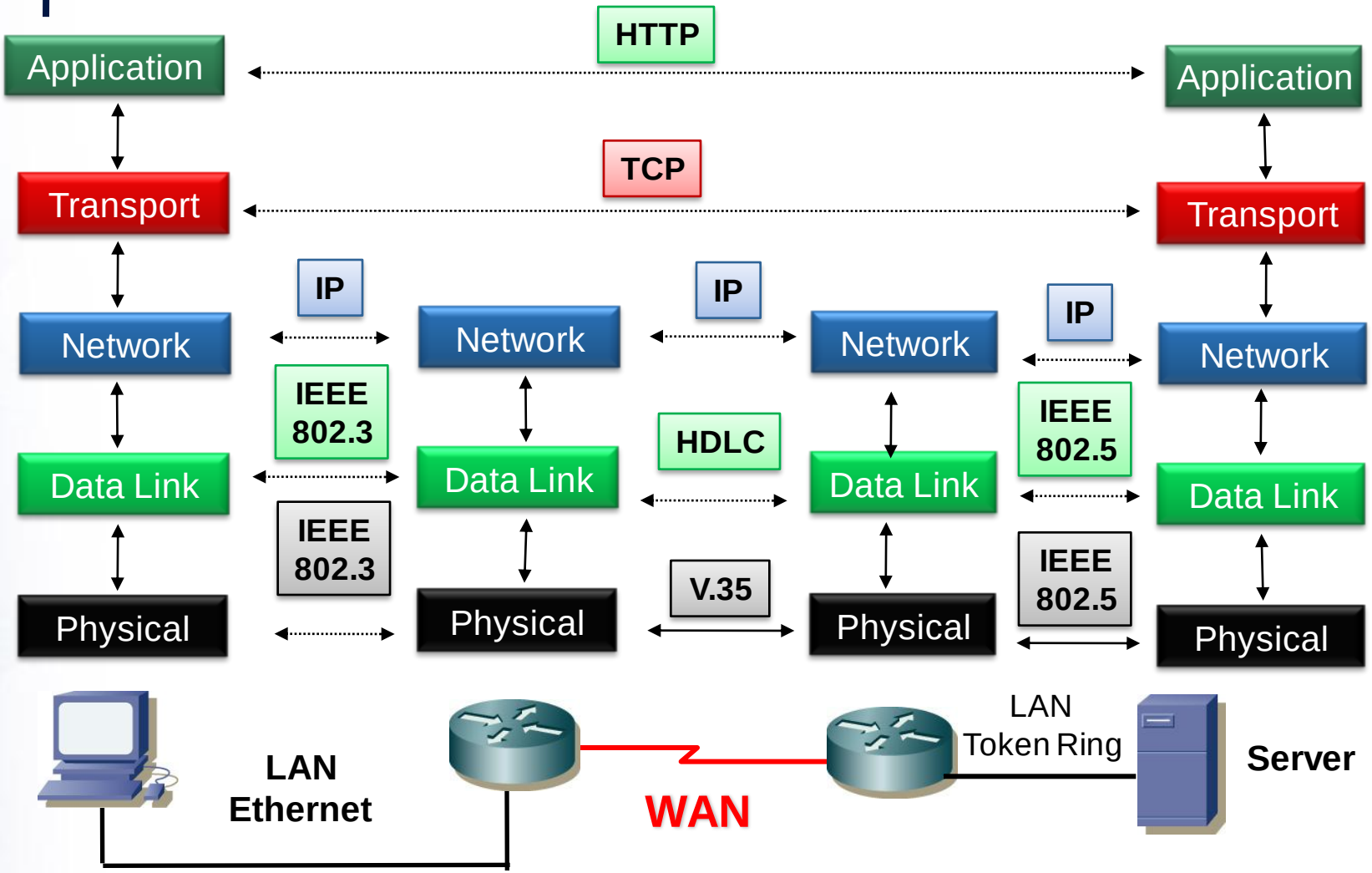
Virtual Private Dial-up Network

- VPN *Remote User* Requirements
  - User Authentication
  - Address Management
  - Data Encryption
  - Multiprotocol Support

Encapsulation vs. Tunneling

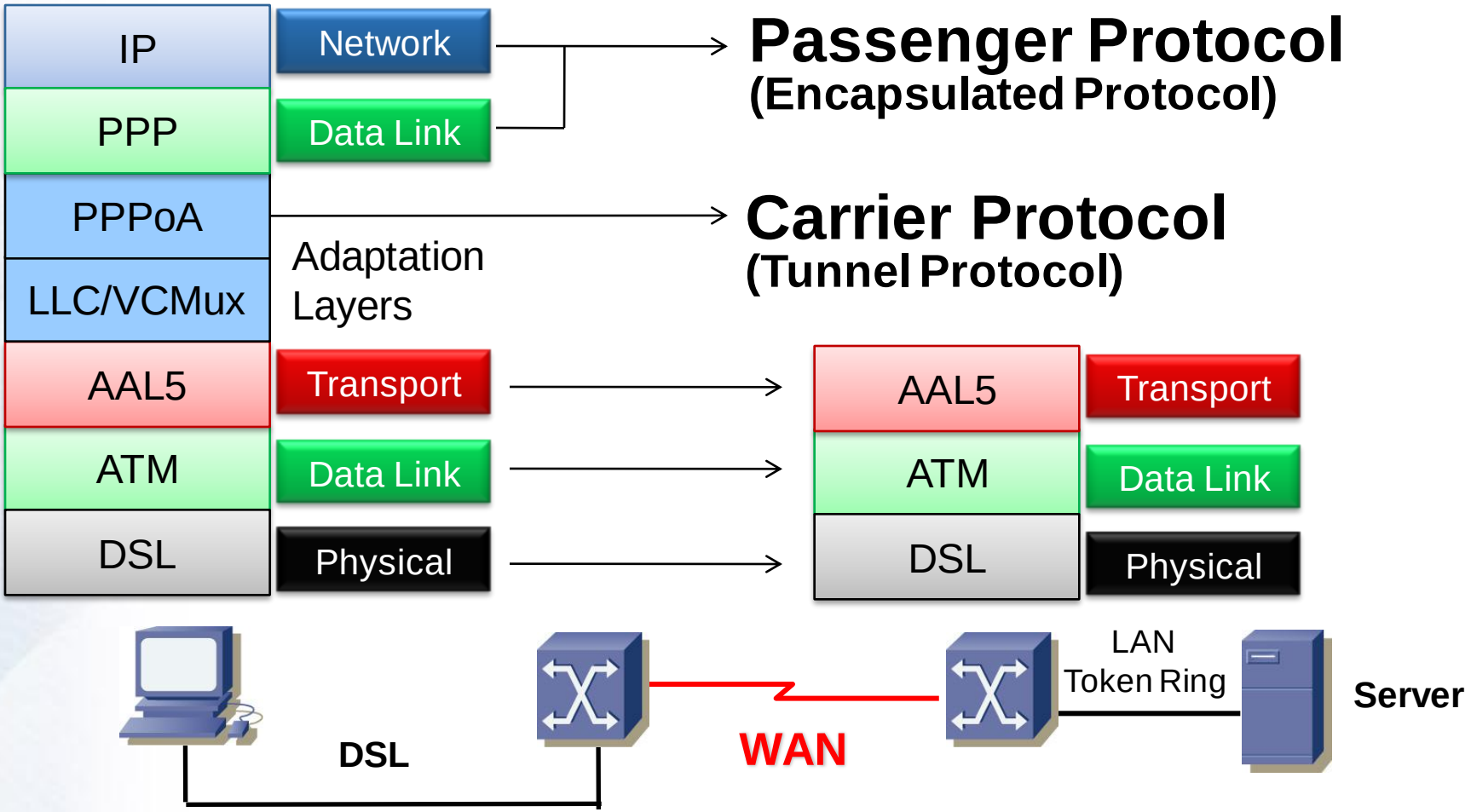
Encapsulation	Tunneling
One or more protocol are stacked but there is only one instance to one layer inside a block	One or more protocol layers are repeated, so that a virtual topology is created on top of the physical topology *[Yuan]*
There is a fixed encapsulation ordering	Any layer can encapsulate any other (Ethernet over TCP possible)

Encapsulation over WAN



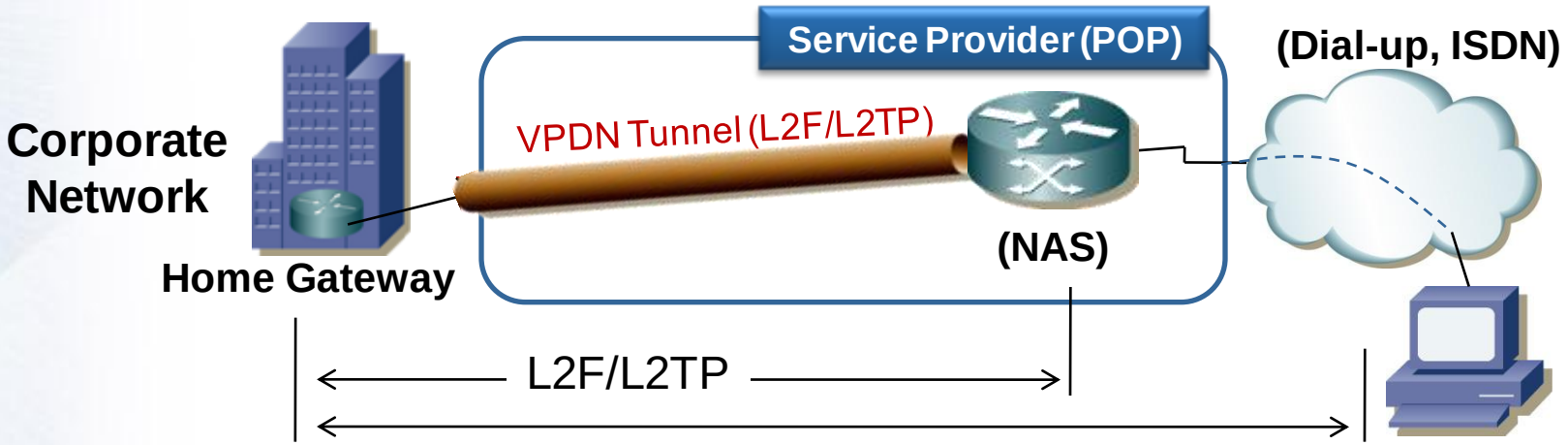
Tunneling DSL

Roles ?



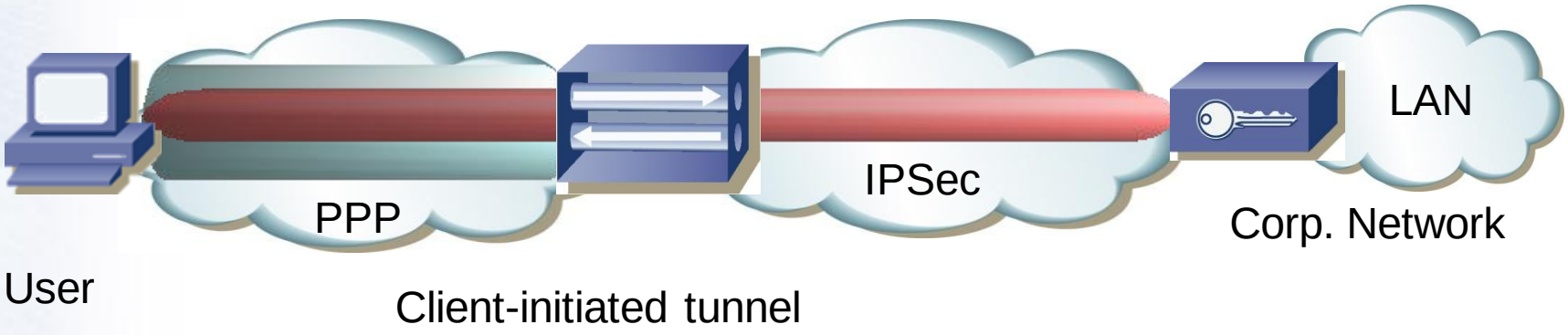
Virtual Private Dial-up Network

- Access of mobile users, home workers, remote offices
- Use of *Layer 2* protocols (*based on PPP*)
  - **PPTP**: Point-to-Point Tunneling Protocol
  - **L2TP**: Layer 2 Tunneling Protocol (RFC 2661)
  - **L2F**: Layer 2 Forwarding (RFC 2341)
- Used over IP networks



Who starts the tunnel? (I)

- **Client-initiated** VPN
  - Known as “voluntary mode”
  - *Point-to-point* connection
  - *End-to-LAN* established
    - VPN Gateway aggregates traffic
    - Used in remote access VPN



Who starts the tunnel? (II)

- Network Access Server (NAS)-initiated VPN
  - Known as “compulsory mode”
  - User aggregation possible
  - Multiple VPNs per user possible

Short Questions

REVIEW QUESTIONS

1. **Describe virtual private networks.**
2. **Define the major VPN topologies.**

Test Questions

1. VPNs emerged as a technology to replace _____.
   - A. Point-to-point connections
   - B. Overlays
   - C. Tag-switched VPNs
   - D. Full-mesh topologies
2. Which of the following is not an overlay VPN topology?
   - A. Full-mesh
   - B. Partial-mesh
   - C. Hub-and-spoke
   - D. Peer-to-peer
3. Which of the following topologies is usually used by financial organizations?
   - A. Full-mesh
   - B. Partial-mesh
   - C. Hub-and-spoke
   - D. Peer-to-peer

Test Questions

4. If optimal routing is desired in a VPN topology, which of the following topologies is the best?
   A. Full-mesh
   B. Partial-mesh
   C. Hub-and-spoke
   D. None of the above
5. In an overlay VPN, a customer router _____ aware of the service provider infrastructure.
   A. Is
   B. Is not
6. In which of the following VPN methods is it the most difficult to implement proper security?
   A. Simple VPN
   B. Overlay
   C. Peer-to-peer
   D. None of the above

Test Questions

7. In a peer-to-peer VPN, a customer router _____ aware of the service provider infrastructure.
   - **A. Is**
   - **B. Is not**
8. Which of the following peer-to-peer VPN methods has the most security problems associated with it?
   - **A. Dedicated router**
   - **B. Shared router**
9. A peer-to-peer VPN offers the same optimal traffic flow as a _____ topology?
   - **A. Full-mesh**
   - **B. Partial-mesh**
   - **C. Hub-and-spoke**
   - **D. None of the above**

Point-to Point Protocol (PPP)

REVIEW

- IP over everything

Medio	RFC	Año
X.25	877, 1356	1983
Ethernet	894	1984
802.x	1042	1988
FDDI	1188, 1390	1990
PPP	1171, 1340, 1332, 1661-1663	1990
Frame Relay	1490	1993
ATM	1483, 1577	1994

Point-to Point Protocol (PPP)

REVIEW

- Link layer protocol **widely** used in the Internet for,
  - Dedicated lines, point-to-point
  - Analogical and digital connections (ISDN)
  - High speed connection over SONET/SDH
- It is able to work in asynchronous and synchronous mode
- *Multiprotocol*, it is able to transport several network protocols simultaneously

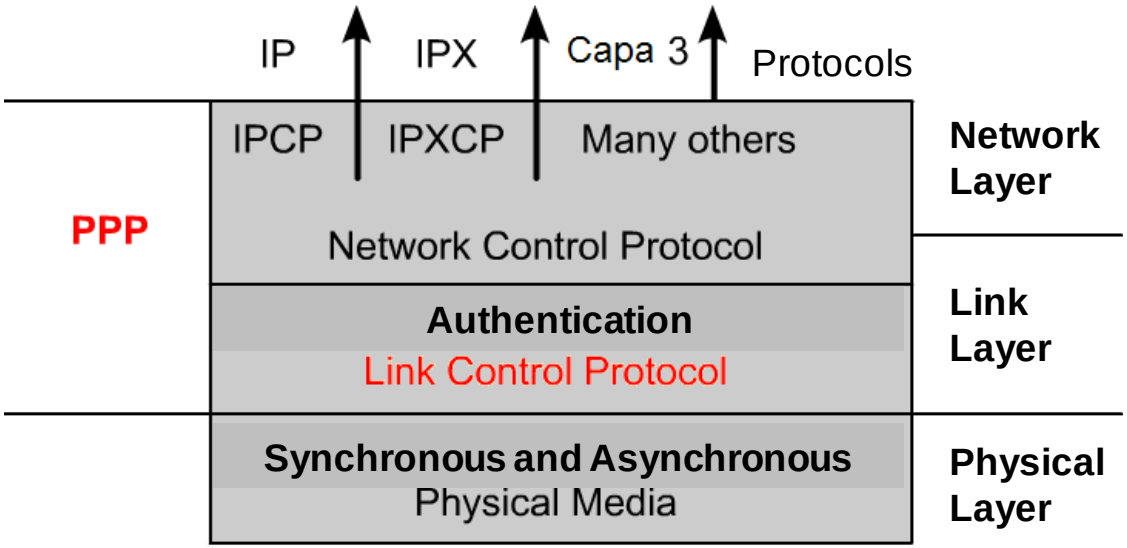
8 bits	12 bits	24 bits	40 bits	*Variable*	16-32 bits
Flag	Address	Control	Protocol	Information	FCS

[RFC 1661, RFC 2153]

PPP Components

REVIEW

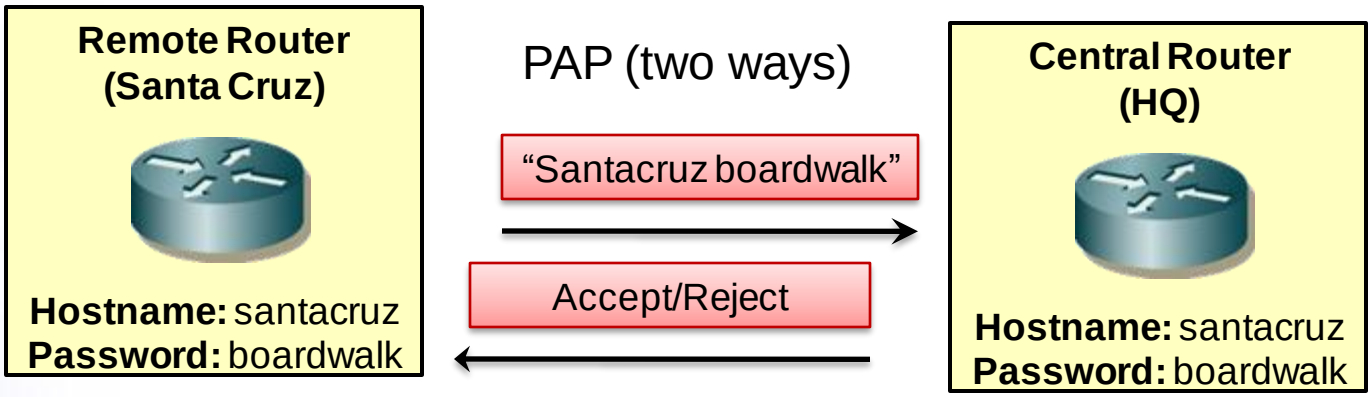
- Phase: “Link Establishment”:
  - LCP listening mode *(C023h → LCP)*
  - Negotiation of extra options *(C023h → LCP)*
  - Check link quality *(C025h → **L**ink **Q**uality **R**eport)*
  - Network layer configuration *(C0__h → NCP)*
  - Link establishment
  - LCP finish
- Phase: Authentication
  (C021h → PAP) or
  (C223h → CHAP)
- Phase: Network layer



PPP Authentication (I)

REVIEW

- Password Authentication Protocol (PAP)

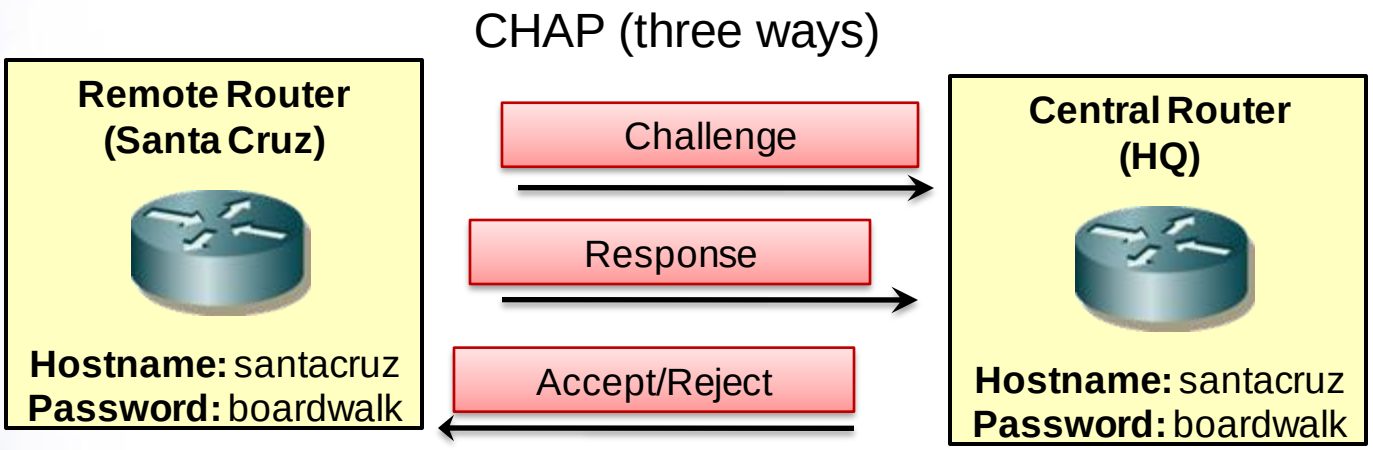


- Passwords are sent in clear text
- No Authentication fail control
- Not secure enough

PPP Authentication (II)

REVIEW

- Challenge Handshake Authentication Protocol (CHAP)

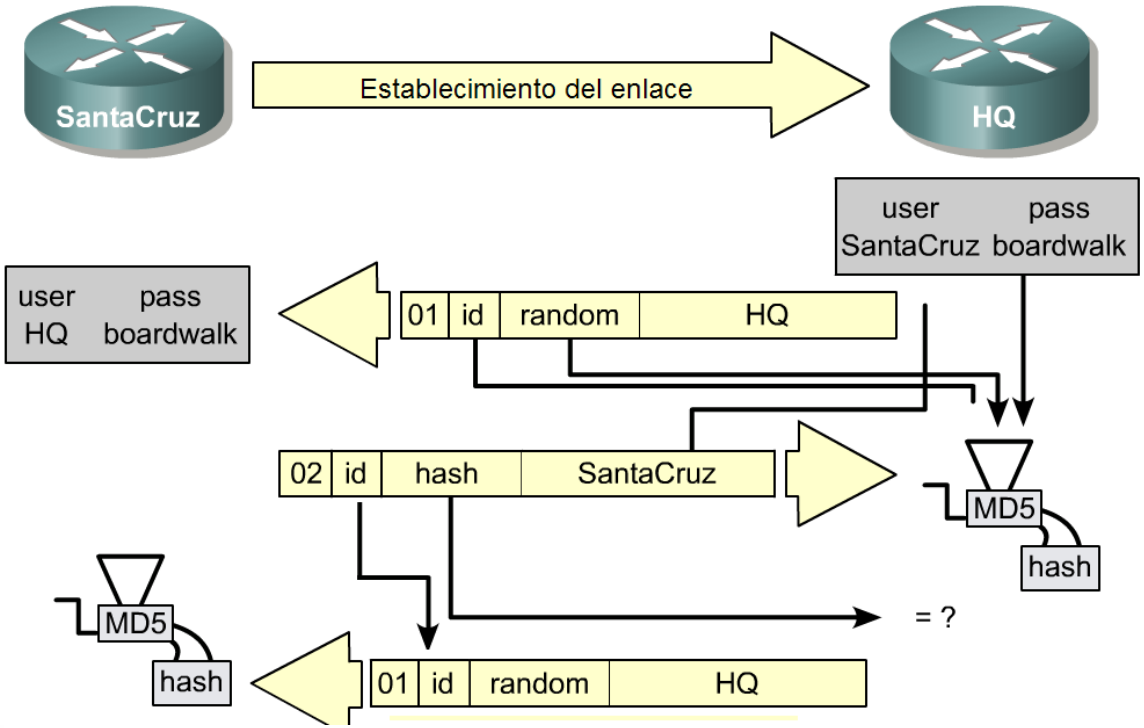


- Passwords are sent over the network
- Passwords agreed *a priori*
- Initial password check followed by periodic checks

PPP Authentication (III)

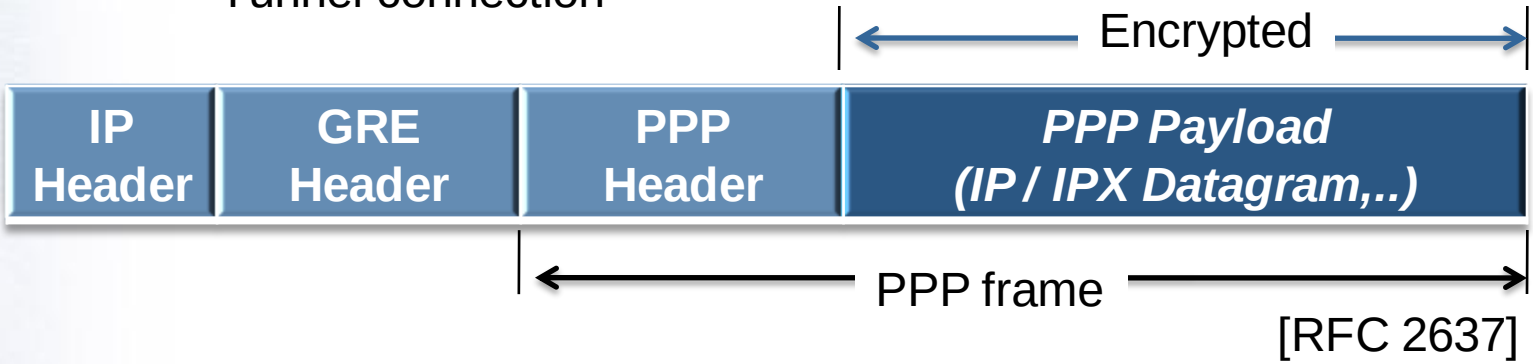
REVIEW

- Challenge Handshake Authentication Protocol (CHAP)



Point-to Point Tunneling Protocol (PPTP) - L2 VPNs

- Point-to-Point Tunneling Protocol (PPTP)
  - Mainly implemented and used by Microsoft
  - Extension of PPP
  - Allows tunneling of PPP datagrams over IP networks
  - Easy to use and to implement
  - Use of 2 connections
    - Control connection
    - Tunnel connection



Point-to Point Tunneling Protocol (PPTP) - L2 VPNs

- Features:
  - Compression
  - Encryption
  - User Authentication
  - Data delivery
- Point-to-Point Tunneling Protocol (PPTP) Protocol implemented by
  - Uses Generic Routing Encapsulation (GRE) PPP frames
  - PPTP-Access-Concentrator (PAC) and PPTP-Network-Server (PNS)
  - Many sessions multiplexed on a single tunnel

PPTP Phases

- PPTP Phase 1
  - LCP used to initiate connection (MPPE,MPPC)
- PPTP Phase 2
  - Authentication to server (MS-CHAP, PAP, EAP,..)
- PPTP Phase 3
  - Callback functions (Callback Control Protocol)
- PPTP Phase 4
  - Protocols negotiated in Phase 1 invoked and setup of PPP connection

PPTP Components

- PPTP Access Concentrator (PAC)
  - Device terminating remote access session
  - In PPTP is the remote user
  - Establishes secure connection to a server and tunnels data
- PPTP Network Server (PNS)
  - Terminates tunnel from the PAC
  - Takes packets from pack, verifies and decrypts

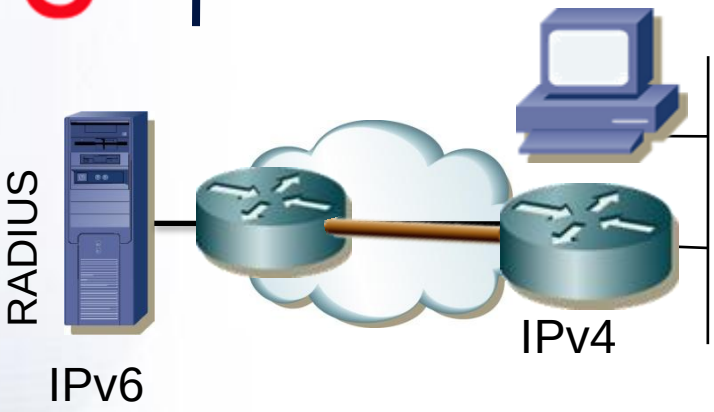
Generic Routing Encapsulation

REVIEW

- GRE encapsulates packets inside IP tunnels
- It is an stateless protocol
- Sequencing of packets
- Useful for some higher-layer protocols
- Priority policies
- Traffic policies

Generic Routing Encapsulation

REVIEW



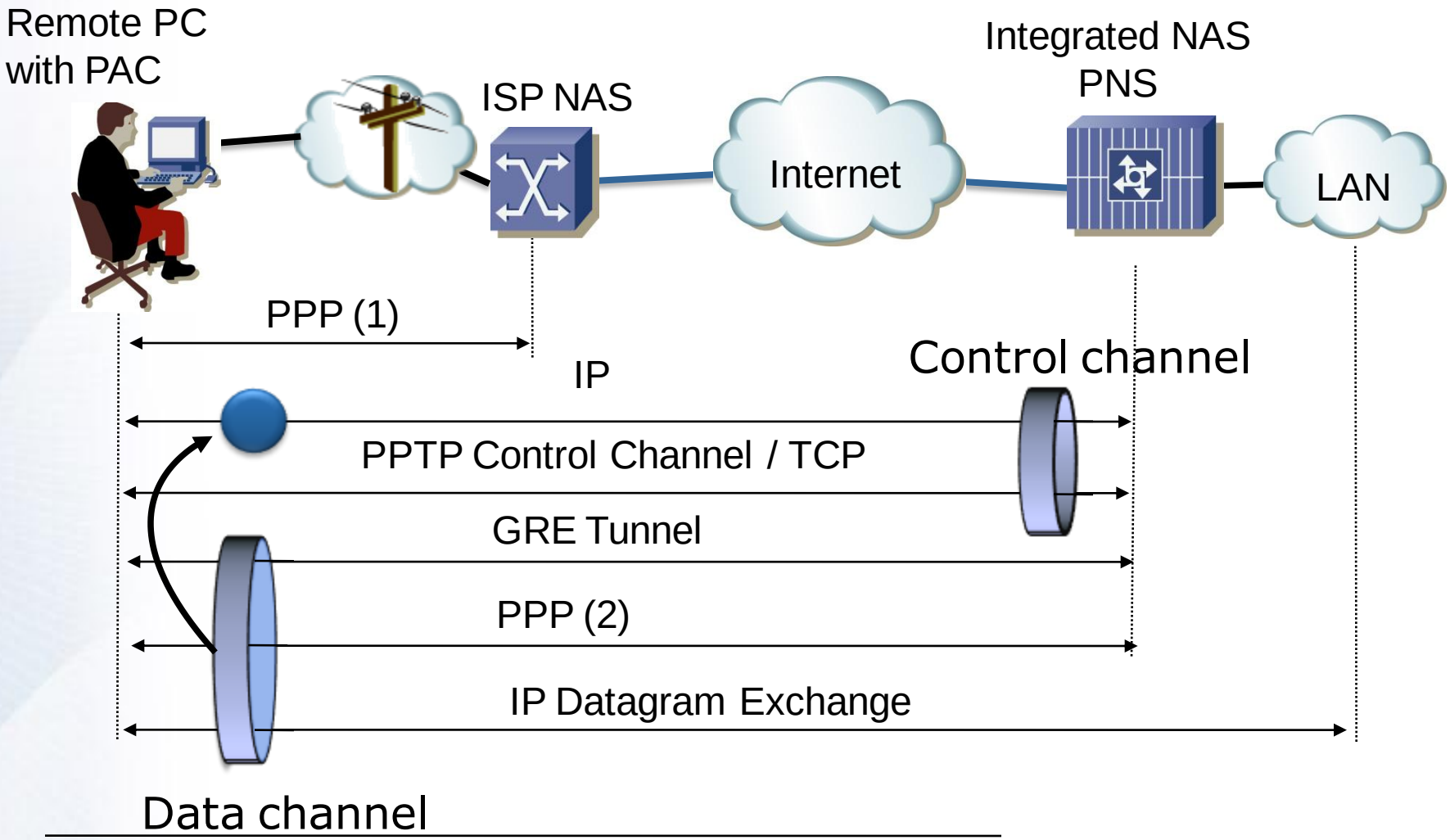
PPTP Operation

- **Control connection (TCP)**
  - Establishing, maintaining and tear down tunnel
  - Connection established from PAC or PNS
  - Message types: (1) Control and (2) Management
- Set-up control connection:
  - (1) Start-Control-Connection-Request / (2) -Reply
  - Collision can be produced → higher IP address wins
- Maintain connection:
  - (1) Echo –Request / (2) –Reply
- Terminating connection:
  - (1) Stop-Control-Connection-Request / (2) -Reply

PPTP Operation

- **Tunnel Connection (GRE)**
  - Carries all user PPP packets
  - Negotiates: PAC address, encryption & compression
- Setup tunnel connection:
  - (1)Outgoing-Call –Request (2)–Reply
  - (3)Incoming-Call –Request (4)–Reply,(5)-Connected
- Encapsulating payload:
  - Enhance GRE used to encapsulate PPP
  - GRE encapsulate into IP
  - Enhanced GRE → sliding window for flow control

PPTP operation



Issues with PPTP

- Fragmentation problems
  - MTU PPP (1532 Bytes) + GRE header (16 bytes) + IP header (20-60 bytes) = 1608 bytes + L2 Hdr
  - If > 1500 → Maybe fragment = decrypt
- Security Concerns (PAC→PNS)
  - No protection for IP, GRE and PPP header
  - Weak encryption
- Address Translation issues
  - NAT or PAT problems may arise

Layer 2 Forwarding (L2F)

L2 VPNs

- Layer 2 Forwarding (L2F)
  - Developed by CISCO
  - Allows multiple tunnels and multiple connections on every tunnel
  - Tunneling PPP and SLIP frames
  - Supports UDP, Frame Relay, X.25

Layer 2 Forwarding (L2F)

L2 VPNs

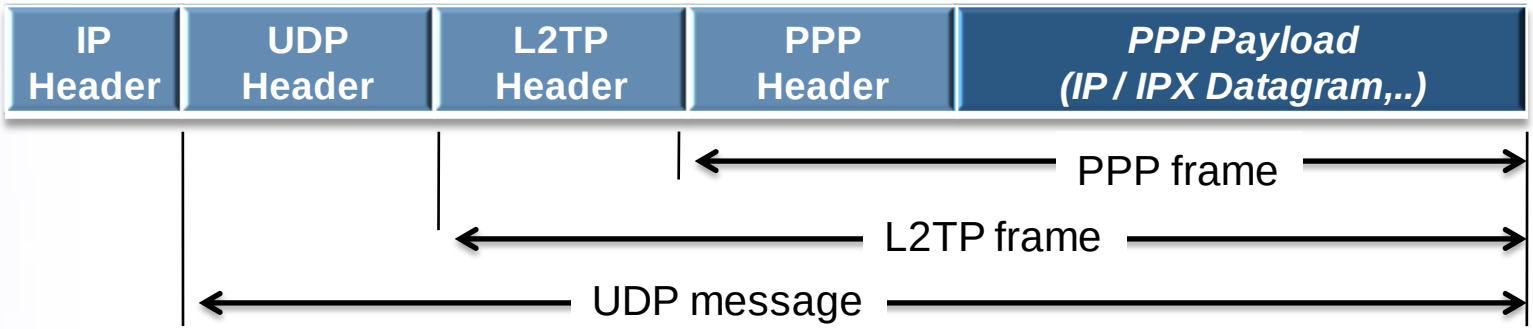
- Establishing connection:
  1. Remote user initiates PPP connection to ISP
  2. ISP undertakes authentication via CHAP or PAP
  3. No tunnel exists:
     - Tunnel will be created

  Tunnel exists:
     - New multiplex ID will be allocated -> notification to home gateway
     - Home gateway accepts or declines new connection

Layer 2 Tunneling Protocol (L2TP) - L2 VPNs

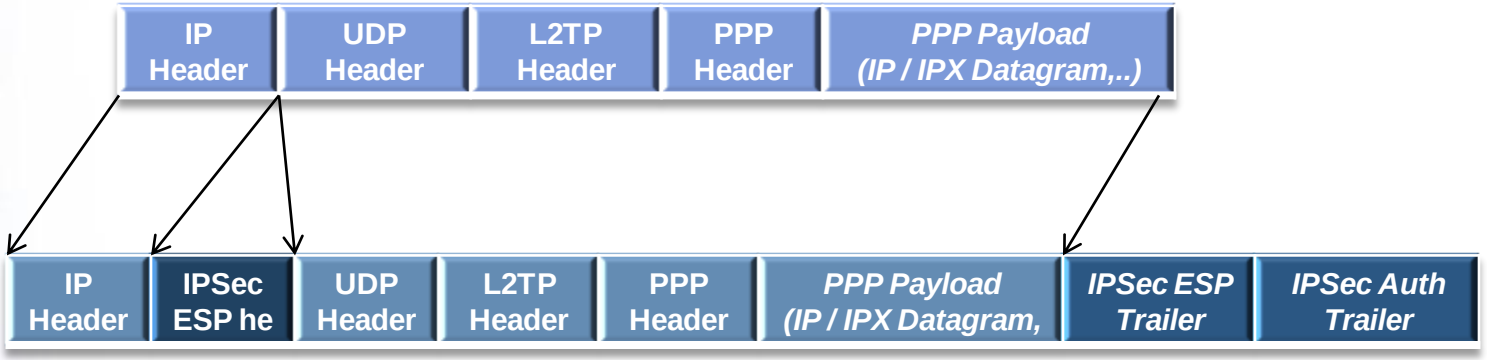
- Layer 2 Tunneling Protocol (L2TP)
  - Combines best features of L2F and PPTP
  - Uses UDP
  - Can be transported over Frame Relay, ATM, X.25
  - Allows multiple tunnels with multiple sessions inside every tunnel
  - Commonly used with IPSec → L2TP/IPSec

[RFC 2661]



L2TP/IPSec - L2 VPNs

- Structure of L2TP/IPSec



Example L2TP/IPSec - L2 VPNs

1. Client Router starts a connection to VPN Server
   - Negotiation starts (using IKE & VPN Server)
   - Agreement on: Authentication method, session keys
   - Certificates exchanges between machines
2. Check certificates using CA and tunnel negotiation
   - Once tunnel is agreed, negotiate PPP connection
3. VPN Server transmits credentials and authentication parameters to RADIUS Server
   - RADIUS Server validates user in the network.
   - RADIUS sends to NAS the information relative to the new admitted user

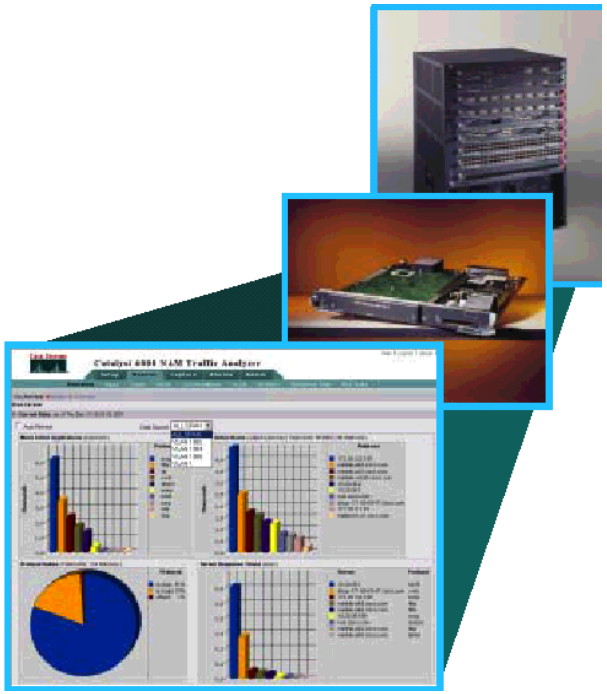
L2TP/IPSec vs. PPTP

PPTP	L2TP/IPSec
Data Encryption after PPP connection establishment	Data encryption begins before connection is established by negotiating an IPSec Security Association (SA)
Use Microsoft Point-to-Point Encryption (MPPE) → stream cipher using RSA RC-4 (40, 56, 128 Bits)	Use Data Encryption Standard (DES) or 3-DES → block cipher (56 Bits)
Requires only user-level authentication	User-level and computer-level authentication
Still implemented in Windows	VPN Client software needed

Table of Contents

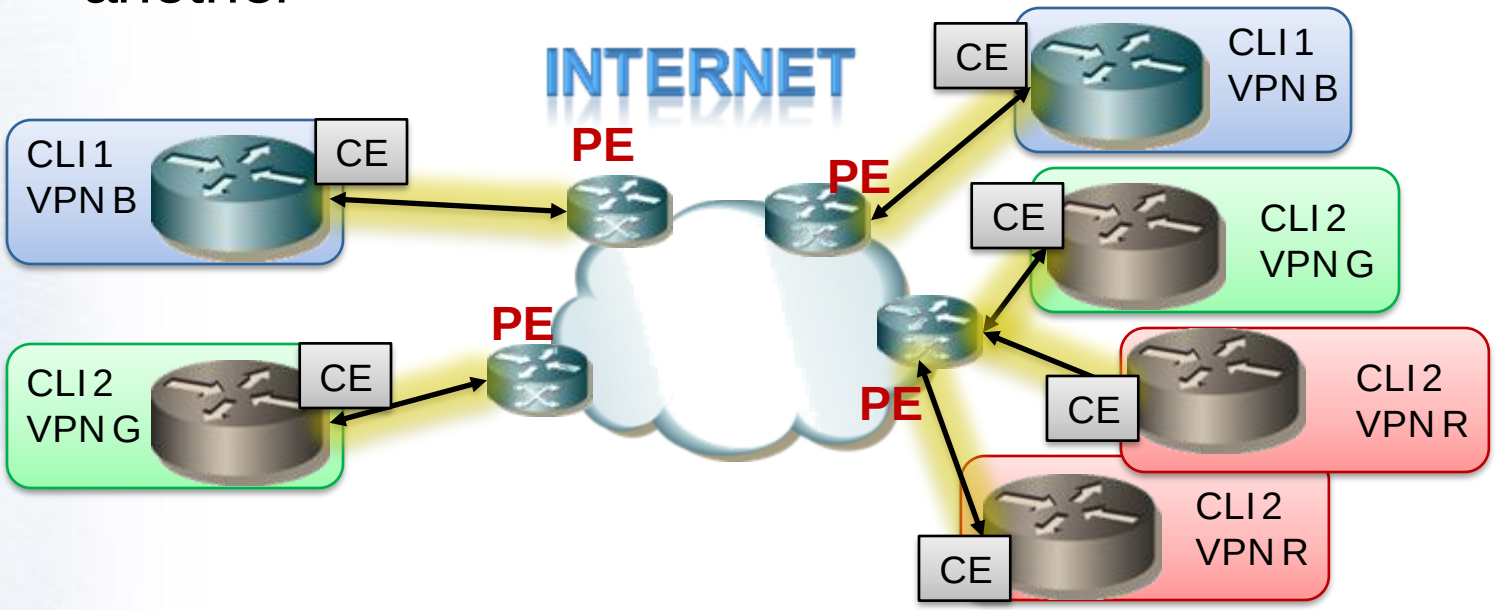
- Overlay VPNs
- **Peer-to-peer VPNs**
- Overlay vs P2P VPNs

- Review Questions



Characteristics of P2P VPNs

- Customer router peers with a service provider device instead of with another customer device
- With a traditional overlay VPN, the customer and service provider networks were well isolated from one another



Why P2P VPNs?

- The peer-to-peer VPN model was introduced a few years ago to alleviate the drawbacks of the overlay VPN model
- Benefits:
  - *Optimal routing:* To get optimal routing with a traditional VPN, you need a full-mesh topology
  - *Routing admin*: Customer only cares about the directly connected PE-router
  - *Addition of new sites simpler:* Only needs to change PE-router config, no new VCs required

Traditional P2P VPNs

- Shared PE-Router
  - Router shared by several customer
  - Isolation by using Access Lists
- Dedicated PE-Router
  - Dedicates routers (virtually)
  - Use of Per-VPN routing tables in PE-router
  - Any routing protocol netween CE- and PE- and BGP between PE- an P-routers

Not only benefits…

- *Security*: Sharing connection with service provider network
- *Management*: Too many routing protocols → Scalability and complexity are compromised
- Constricted IP addresses: Shared address between service provider and customer
- Default routes: Limitation for the use of several ISPs

The solution for P2P VPNs

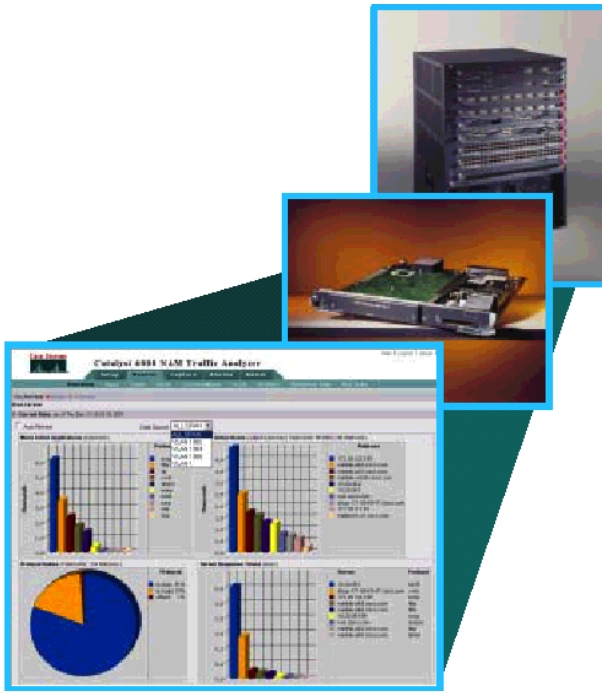
MPLS/VPNs

coming soon….

Table of Contents

- Overlay VPNs
- Peer-to-peer VPNs
- **Overlay vs P2P VPNs**

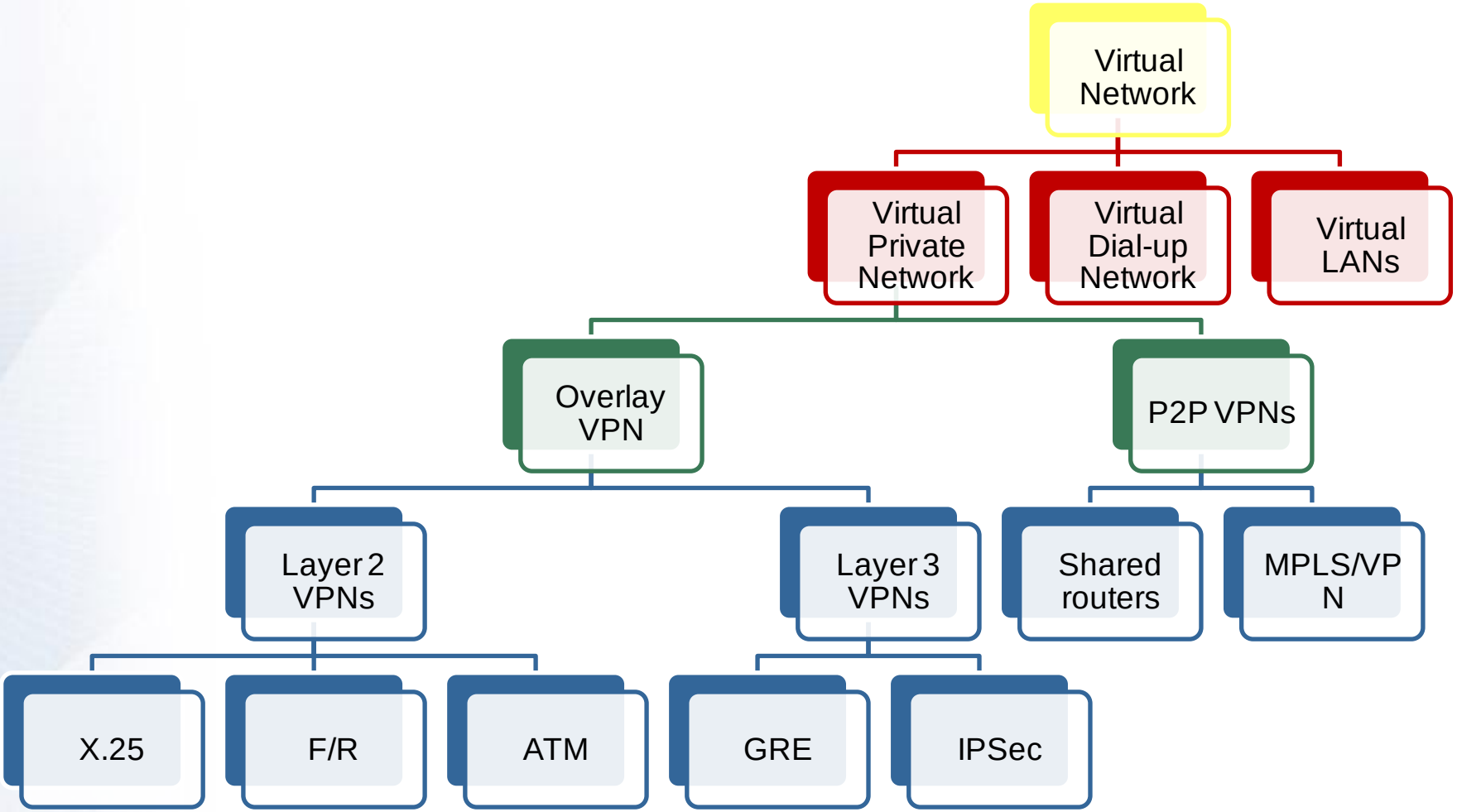
- Review Questions



Comparison of VPNs

	Comment	Layer 2 Virtual Circuits	Layer 3 Tunnels	MPLS VPNs
Ease of setup and management	Must have advanced monitoring and automated flow-through systems to quickly roll out new services, enforce security and QoS policies, and support Service-Level Agreements (SLAs).	Low	Medium	High
Security	Must offer different levels of security, including tunneling, encryption, traffic separation, authentication, and access control.	High	High	High
Scalability	Must be able to scale the provisioning of VPN services from small and medium-sized businesses to large enterprise customers.	Medium	Medium	High
QoS	Must be able to assign priority to mission-critical or delay-sensitive traffic and manage congestion across varying bandwidth rates.	High	Must be implemented using other technologies	High
Provisioning costs	Direct and indirect costs of provisioning the VPNs.	High	Medium	Low

Summary technologies



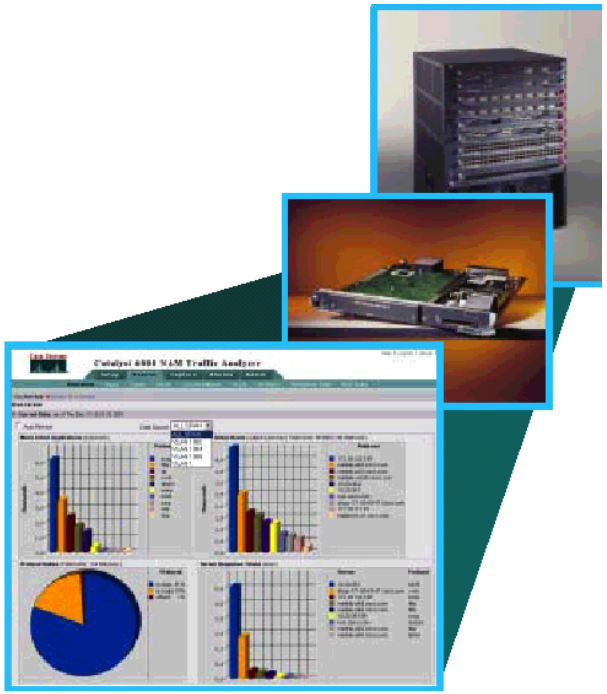
Delivery of Presentation

- A Task will be added on the Moodle (16Jan)
- Content (3 sections - mandatory)
  - Description & Operation of L2F
  - Description & Operation of L2TP
  - IPSec for L2TP
- Presentation per group:
  - 10-12 slides per presentation
  - 15 minutes + questions / group
  - Each group will present only 1 Section

Table of Contents

- Overlay VPNs
- Peer-to-peer VPNs
- Overlay vs P2P VPNs

- **Review Questions**



Short Questions

REVIEW QUESTIONS

3. **Describe peer-to-peer VPNs.**
4. **Compare overlay and peer-to-peer VPNs.**

Test Questions

10. Which of the following overlay VPN topologies is the least expensive to implement?
    - A. Full-mesh
    - B. Partial-mesh
    - C. Hub-and-spoke
    - D. None of the above

11. IPSec and GRE tunnels are Layer _____ VPN technologies?
    - A. 1
    - B. 2
    - C. 3
    - D. 7

12. Which of the following is a Layer 1 VPN technology?
    - A. IPSec
    - B. Frame Relay
    - C. GRE
    - D. ISDN

Test Questions

13. A(n) _____ is where everyone being connected is part of the same company or organization.
    - A. Intranet
    - B. Extranet
    - C. Combination of intranet and extranet
    - D. None of the above
14. A(n) _____ is where sites from different companies or organizations are connected.
    - A. Intranet
    - B. Extranet
    - C. Combination of intranet and extranet
    - D. None of the above
15. Frame Relay and ATM are Layer _____ VPN technologies.
    - A. 1 B. 2
    - C. 3 D. 7

Test Questions

16. Which of the following topologies provides the most redundancy?
    - **A. Full-mesh**
    - **B. Partial-mesh**
    - **C. Hub-and-spoke**
    - **D. None of the above**
17. Which of the following peer-to-peer VPN methods is the most expensive to implement?
    - A. Dedicated router
    - B. Shared router
18. Which of the following overlay VPN topologies is typically used by financial organizations?
    - A. Full-mesh
    - B. Partial-mesh
    - C. Hub-and-spoke
    - D. None of the above

Test Questions

REVIEW QUESTIONS

19. In a peer-to-peer VPN, the _____ becomes responsible for routing protocol convergence.

    A. Customer
    B. Service provider
    C. Edge-LSR
    D. PE

20. Which of the following are valid peer-to-peer VPN methods? (Choose two.)

    A. Dedicated router
    B. Full-mesh
    C. Partial-mesh
    D. Shared router

21. Of the following choices below, only three could be used as WAN encapsulation methods, as opposed to LAN encapsulation. Which three are they? (Choose three)

    A. FDDI B. HDLC C. Frame Relay
    D. PPP E. Token Ring F. Ethernet G. VTP

Test Questions

22. What can the network administrator utilize by using PPP (Point to Point Protocol) as the Layer 2 encapsulation? (Choose three)
    - A. Compression
    - B. QOS
    - C. Sliding windows
    - D. VLAN support
    - E. Authentication
    - F. Multilink support
23. Two routers are connected via a PPP connection. Which of the following are key characteristics of this PPP connection? (Choose three)
    - A. PPP can be used over analog circuits
    - B. PPP encapsulates several routed protocols
    - C. PPP maps Layer 2 to Layer 3 address
    - D. PPP provides error correction
    - E. PPP supports IP only
    - F. PPP provides encryption services

Test Questions

24. In a point to point connection between two TestKing offices, which PPP subprotocol negotiates authentication options?

    A. NCP
    B. ISDN
    C. SLIP
    D. LCP
    E. DLCI

25. Routers R1 and R2 are connected via a private line using PPP. On this link, which of the following options lists the steps in PPP session establishment in the correct order?

    A. network layer protocol phase, optional authentication phase, link establishment phase
    B. link establishment phase, network layer protocol phase, optional authentication phase
    C. optional authentication phase, network layer protocol phase, link establishment phase
    D. link establishment phase, optional authentication phase, network layer protocol phase
    E. network layer protocol phase, link establishment phase, optional authentication phase
    F. optional authentication phase, link establishment phase, network layer protocol phase
    G. None of the above