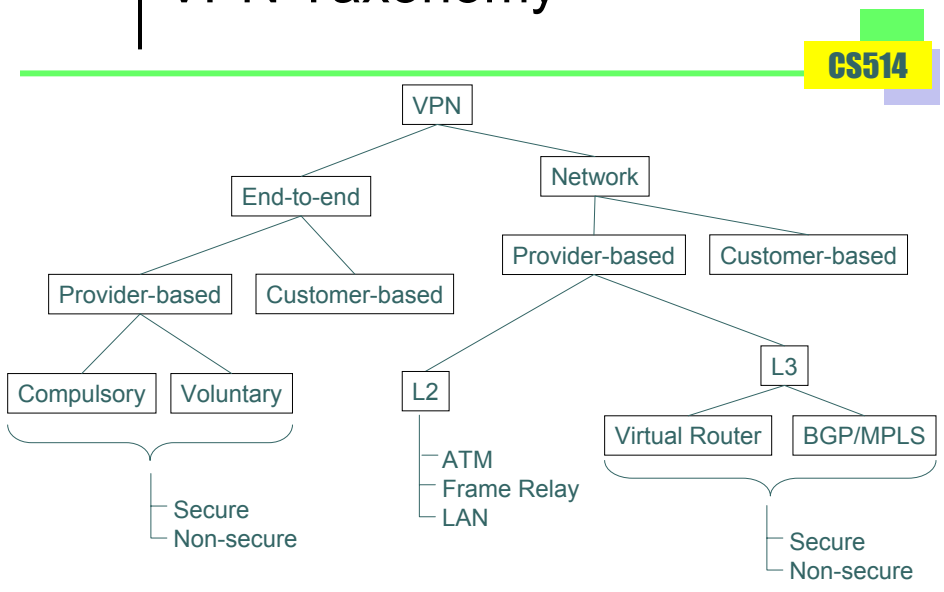
CS514: Intermediate Course in Computer Systems

Lecture 21: Nov 5, 2003

"VPNs and other network-level security concepts"

VPN Taxonomy



What is a VPN?

CS514

- Making a shared network look like a private network
- Why do this?
  - Private networks have all kinds of advantages
    - (we'll get to that)
  - But building a private network is expensive
    - (cheaper to have shared resources rather than dedicated)

History of VPNs

CS514

- Originally a telephone network concept
  - Separated offices could have a phone system that looked like one internal phone system
- Benefits?
  - Fewer digits to dial
  - Could have different tariffs
    - Company didn't have to pay for individual long distance calls
  - Came with own blocking probabilities, etc.
    - Service guarantees better (or worse) than public phone service

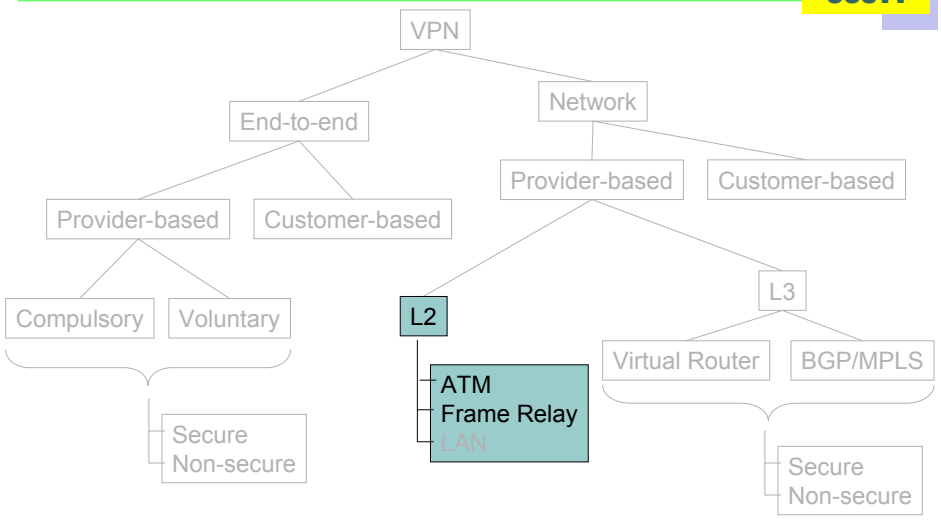
Original data VPNs

CS514

- Lots of different network technologies in those days
  - Decnet, Appletalk, SNA, XNS, IPX, …
  - None of these were meant to scale to global proportions
  - Virtually always used in corporate settings
- Providers offer virtual circuits between customer sites
  - Frame Relay or ATM
  - A lot cheaper than dedicated leased lines
- Customer runs whatever network technology over these
- These still exist (but being replaced by IP VPNs)

VPN Taxonomy

CS514



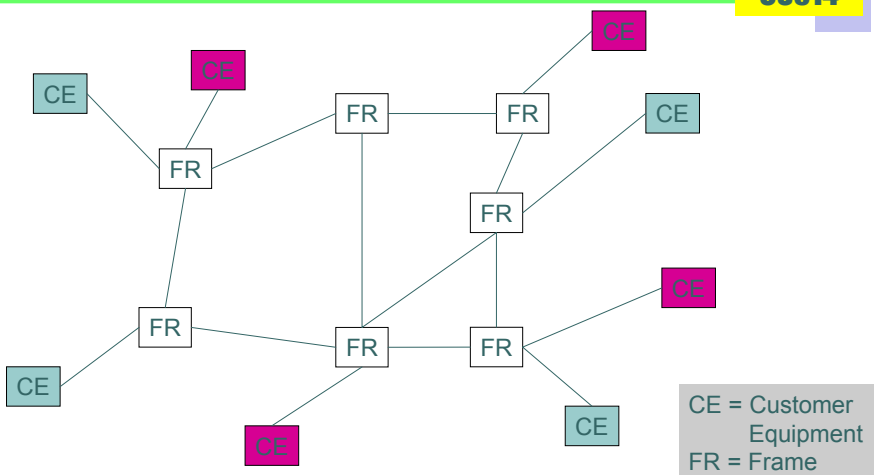
Advantages of original data VPNs

CS514

- Repeat: a lot cheaper than dedicated leased lines
  - Corporate users had no other choice
  - This was the whole business behind frame-relay and ATM services
- Fine-grained bandwidth tariffs
- Bandwidth guarantees
  - Service Level Agreements (SLA)
- “Multi-protocol”

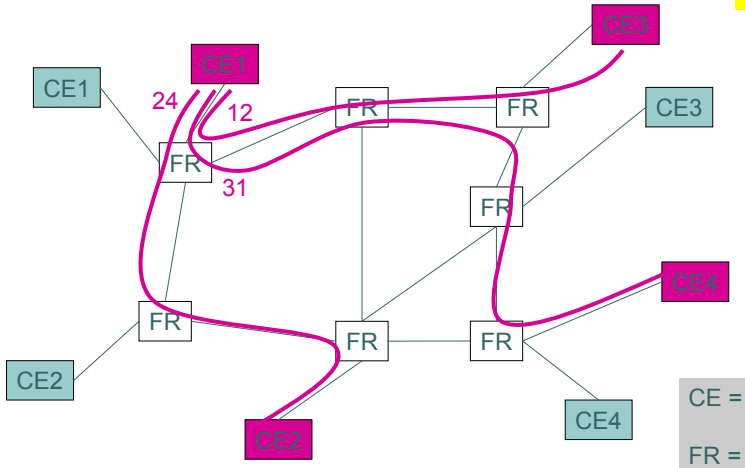
Frame Relay VPN Example

CS514



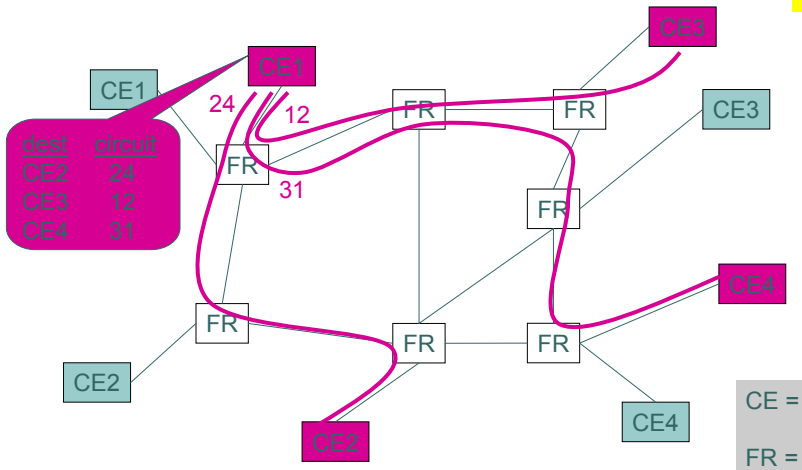
Define circuits CE to CE (for given customer: purple)

CS514



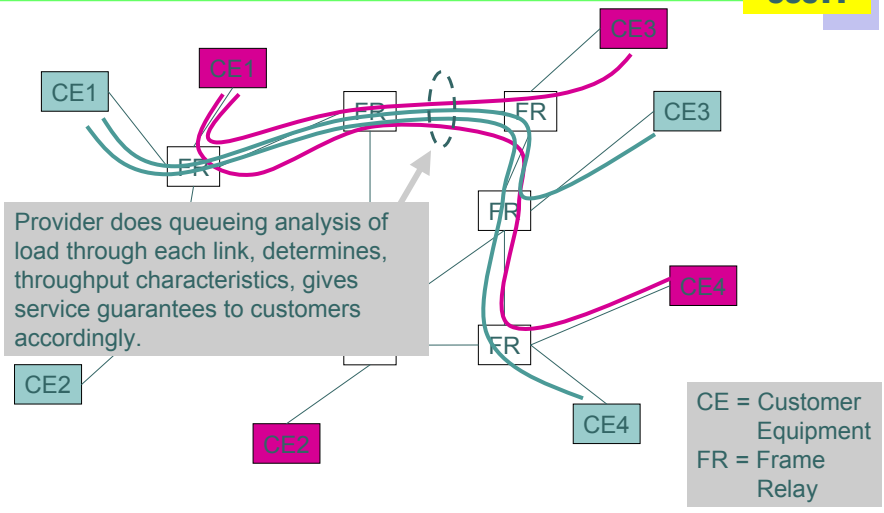
Customer establishes routing tables (per protocol)

CS514



Provider provisions underlying network

CS514



How has the world changed?

CS514

- Everything is IP now
  - Some old stuff still around, but most data networks are just IP
- So, why do we still care about VPNs???

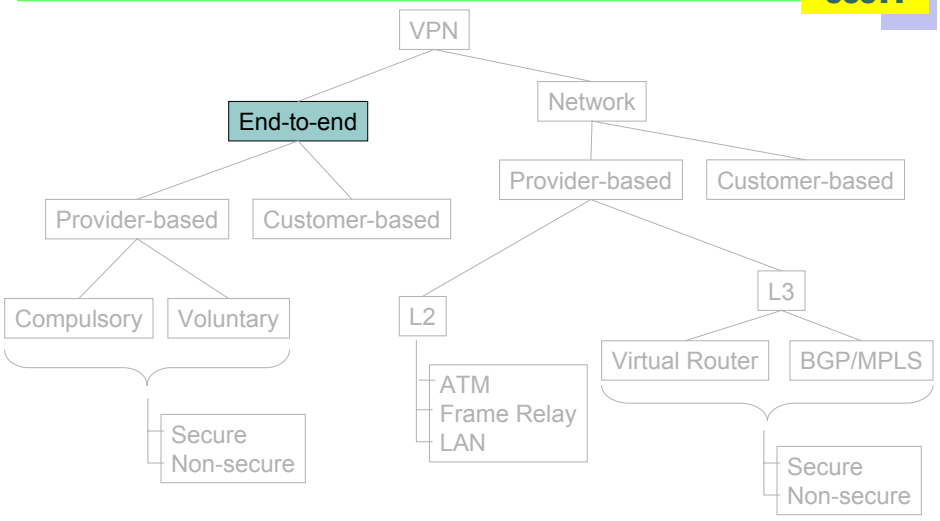
IP VPN benefits

CS514

- IP not really global (private addresses)
  - VPN makes separated IP sites look like one private IP network
- Security
- Bandwidth guarantees across ISP
  - QoS, SLAs
- Simplified network operation
  - ISP can do the routing for you

End-to-end VPNs

CS514



End-to-end VPNs

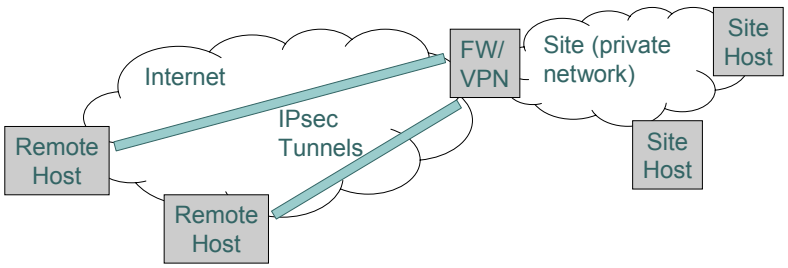
CS514

- Solves problem of how to connect remote hosts to a firewalled network
  - Security and private addresses benefits only
  - Not simplicity or QoS benefits

End-to-end VPNs

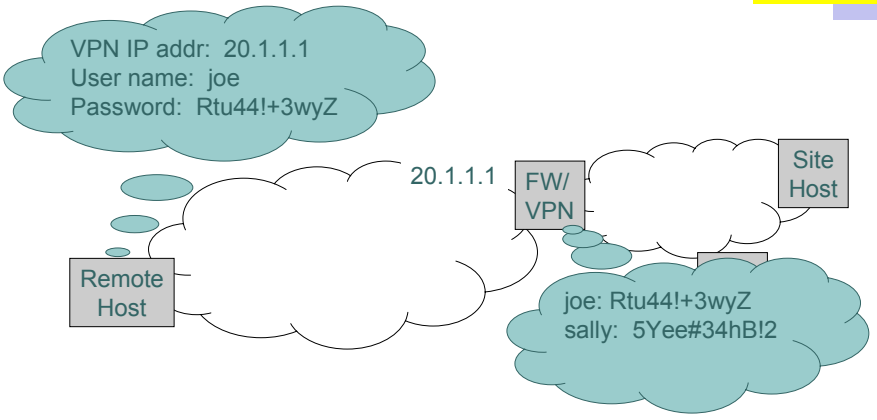
CS514

- Solves problem of how to connect remote hosts to a firewalled network



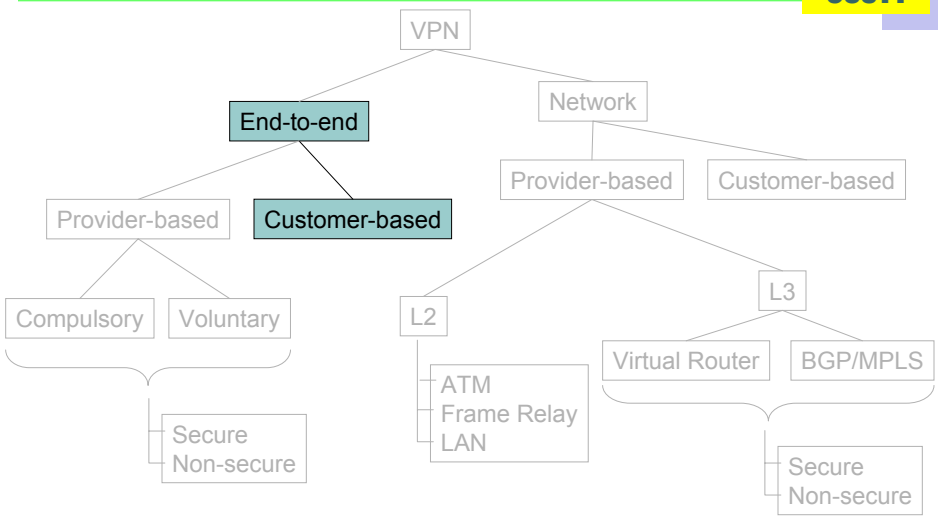
End-to-end VPNs: Configuration

CS514



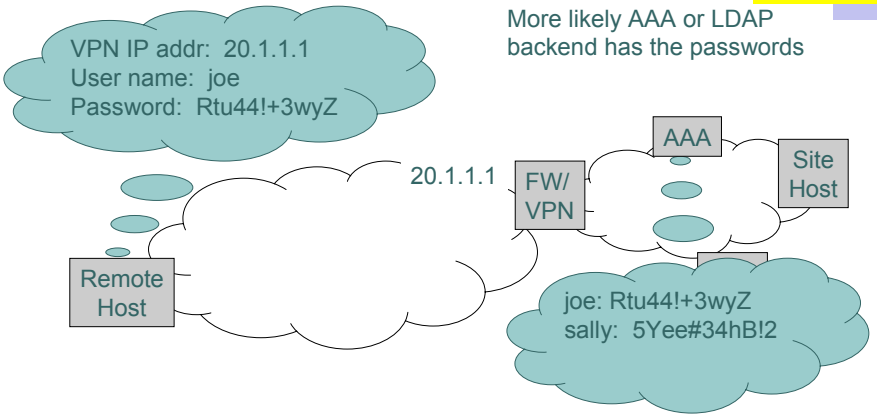
End-to-end VPNs

CS514



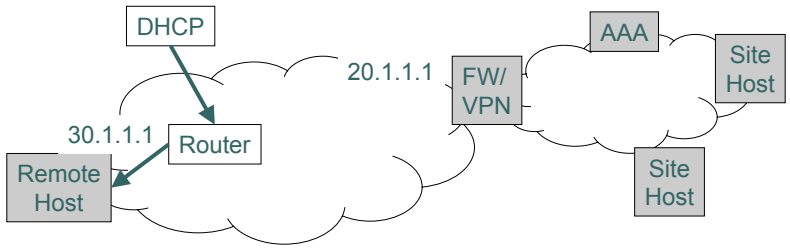
End-to-end VPNs: Configuration

CS514



End-to-end VPNs: Host gets local IP address

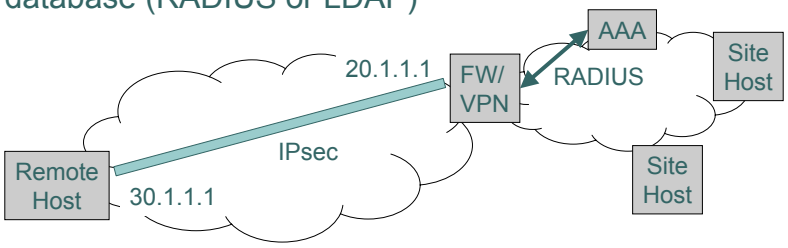
CS514



End-to-end VPNs: Host connects to VPN

CS514

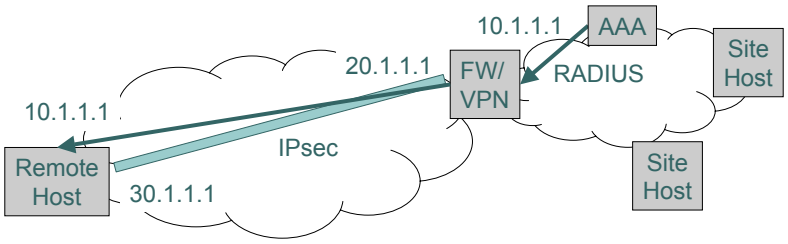
VPN authenticates remote host through backend database (RADIUS or LDAP)



End-to-end VPNs: VPN assigns site address

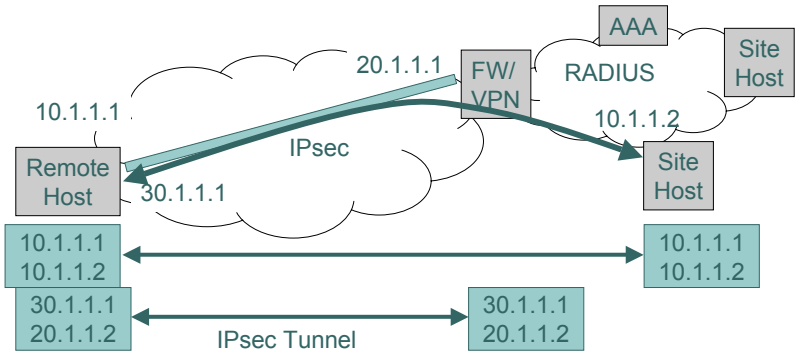
CS514

As proprietary enhancement to IPsec, or with PPP (over IPsec)



End-to-end VPNs: Packets tunneled over IPsec

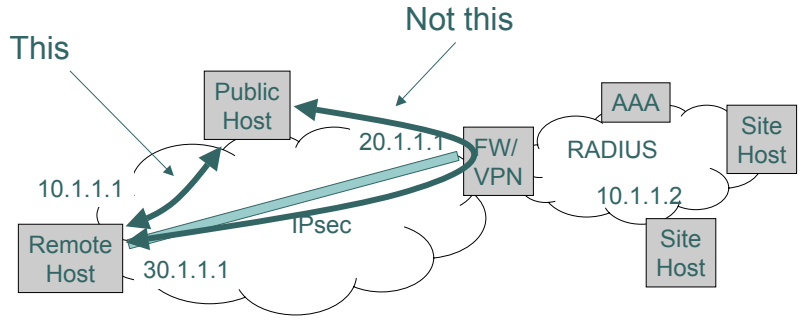
CS514



End-to-end VPNs: Packets tunneled over IPsec

CS514

Some VPN clients smart enough to avoid sending non-VPN traffic through the VPN tunnel



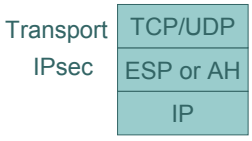
IPsec

CS514

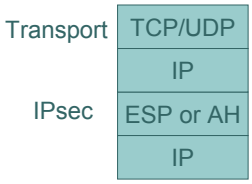
- Two parts: Session Establishment (key exchange) and Payload
- IKE/ISAKMP is session establishment
  - Negotiate encryption algorithms
  - Negotiate payload headers (AH, ESP)
  - Negotiate policies
- Payloads
  - AH: Authentication Header
    - Authenticates each packet but doesn't encrypt
    - Has fallen out of favor (redundant and no more efficient, and doesn't work with NAT)
  - ESP: Encapsulating Security Payload
    - Encrypts (with authentication as side effect)

IPsec transmission modes: Transport or Tunnel mode

CS514



Transport mode. Used when IPsec tunnel is end-to-end.



Tunnel mode. Used when IPsec tunnel not end-to-end. Hides the IP identity of endpoints.

New IPsec transmission modes

CS514

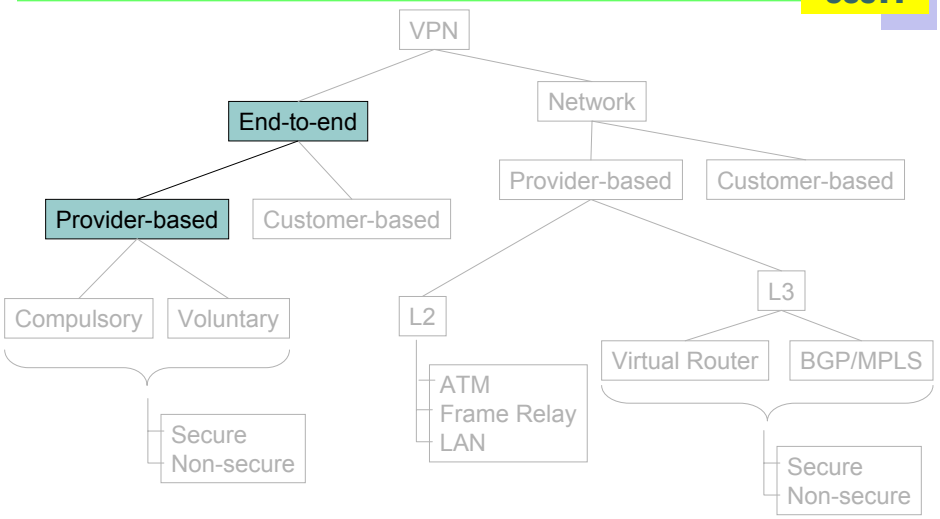
Transport	TCP/UDP
IPsec	ESP or AH
NAT	UDP
	IP

Extra layer of UDP allows IPsec to work over NAT.

Transport	TCP/UDP
	IP
IPsec	ESP or AH
NAT	UDP
	IP

End-to-end VPNs

CS514

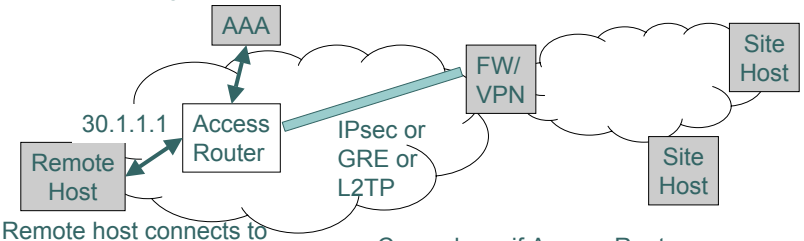


End-to-end VPNs: Host gets local IP address

CS514

2. If PPP, AAA tells Access Router to tunnel user to VPN. (If not PPP, Access Router uses local configuration.)

3. Tunnel pre-established (or packets forwarded over pre-established tunnel)



1. Remote host connects to Internet (dialup-PPP or PPPoE (cable) or DSL)

Compulsory if Access Router forces tunnel, voluntary if user requests it (through certain NAI). NAI = “user@domain”

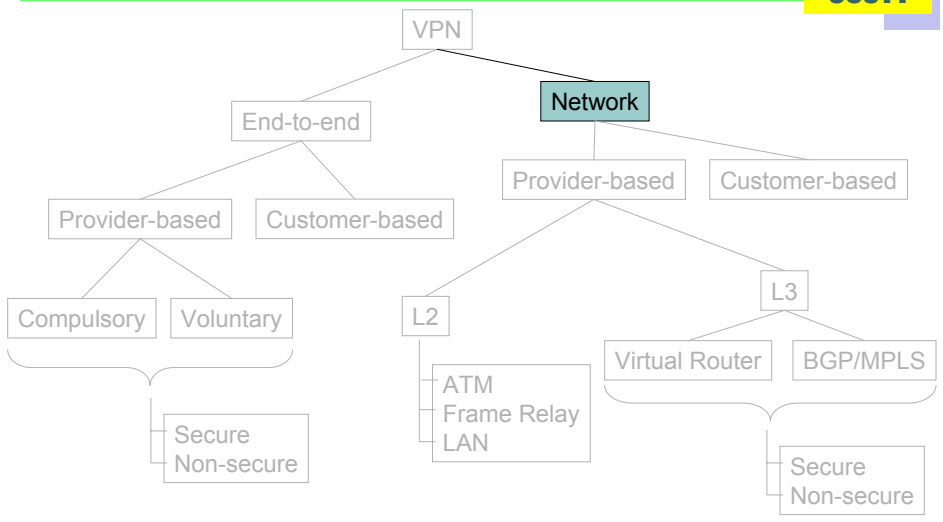
Provider-based end-to-end VPNs

CS514

- Used for instance when enterprise pays for employee access, wants it to go through enterprise network
  - I know Cisco did this
  - But never used that much
    - Business model didn’t take off
  - Used even less now
    - In part because VPN client comes with windows OS???
- The tunneling technology commonly used for roaming dialup though

Network VPNs

CS514



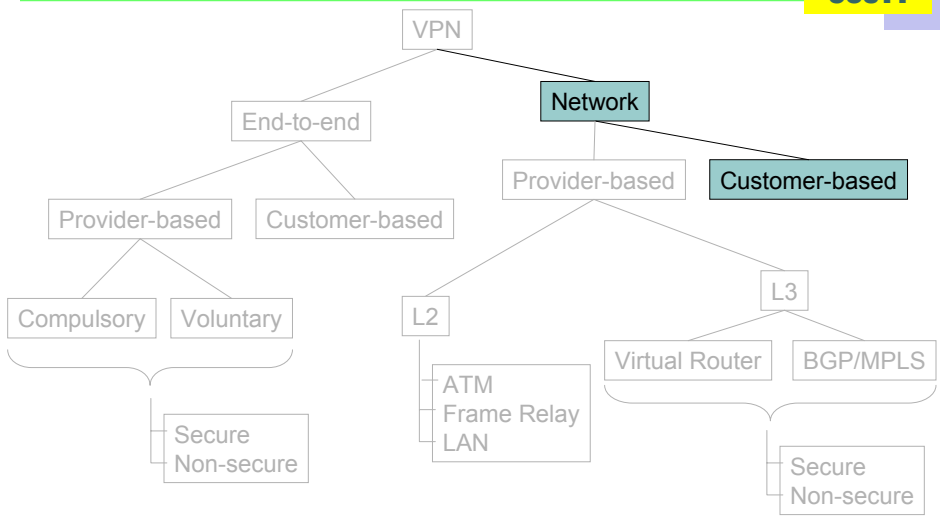
Reiterate network VPN benefits

CS514

- Makes separated IP sites look like one private IP network
- Security
- QoS guarantees
- Simplified network operation

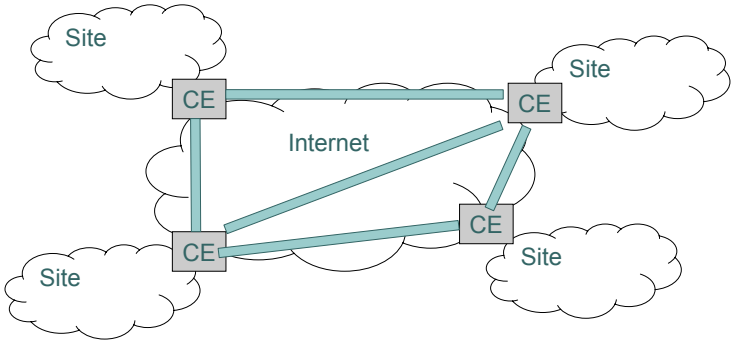
Customer-based Network VPNs

CS514



Customer-based Network VPNs

CS514



Customer buys own equipment, configures IPsec tunnels over the global internet, manages addressing and routing. ISP plays no role.

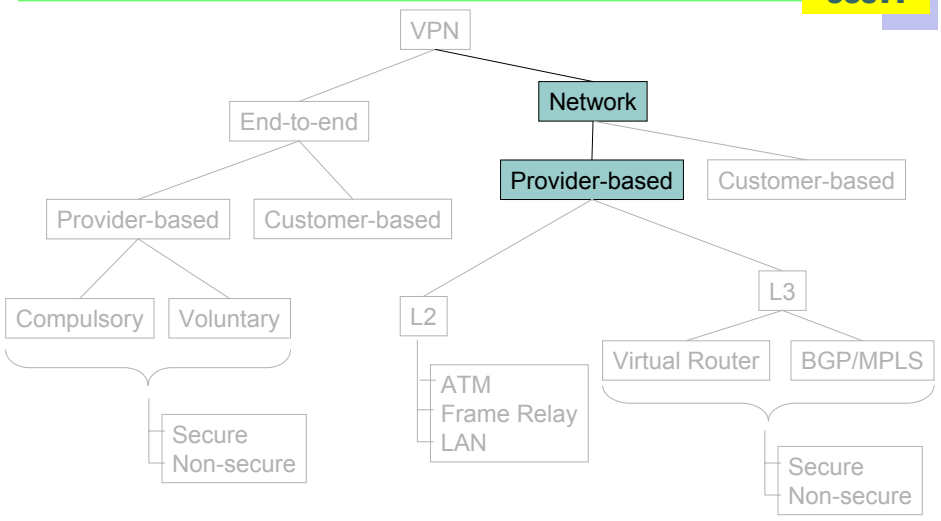
Customer-based Network VPNs

CS514

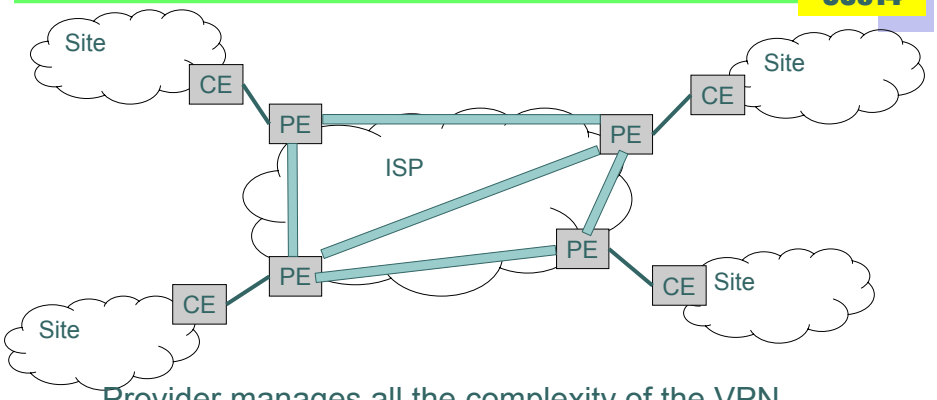
- Great for enterprises that have the resources and skills to do it
  - Large companies
- More control, better security model
  - Doesn't require trust in ISP ability and intentions
  - Can use different ISPs at different sites
- But not all enterprises have this skill

Provider-based Network VPNs
(aka Provider Provisioned: PPVPN)

CS514

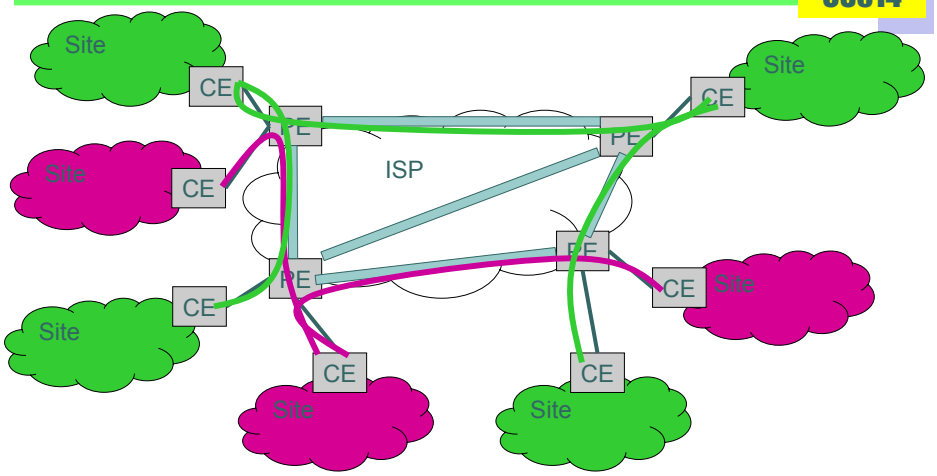


Provider-based Network VPNs



Provider manages all the complexity of the VPN.
Customer simply connects to the provider equipment.

Same provider equipment used for multiple customers



Model for customer

CS514

- Attach to ISP router (PE) as though it was one of your routers
- Run routing algorithm with it
  - OSPF, RIP, BGP
- PE will advertise prefixes from other sites of same customer

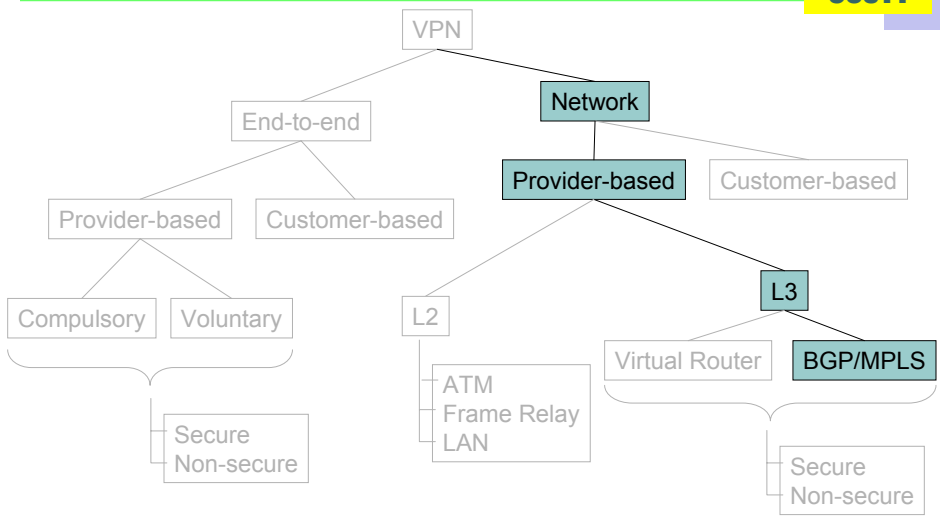
Various PPVPN issues

CS514

- Tunnel type?
  - IPsec (more secure, more expensive)
  - GRE etc.
- How to discover which customer is at which PE?
  - Don't want PEs without given customer to participate in routing for that customer
- How to distinguish overlapping private address spaces

BGP/MPLS VPNs (RFC2547)

CS514



BGP/MPLS VPNs (RFC2547)

CS514

- Cisco invention
  - Leverage Cisco's investment in both BGP and MPLS (Multi-Protocol Label Switching)
- What is MPLS?
  - Link-layer technology
    - Tags like circuit switching
    - But with some IP awareness
  - How Cisco killed Epsilon
  - Initially marketed as high performance switching
  - Later became "traffic engineering" and VPN

Why is MPLS needed for IP traffic engineering?

CS514

- Good question---not everybody agrees with this
- Traffic engineering means to manipulate which links traffic goes over to meet SLAs
- To do this with routers requires looking at both source and dest IP
  - Routers don't do this (they could, but they don't)
  - Complex to manage
- But one (reasonable) school of thought says just over-provision and forget about (micro) traffic engineering

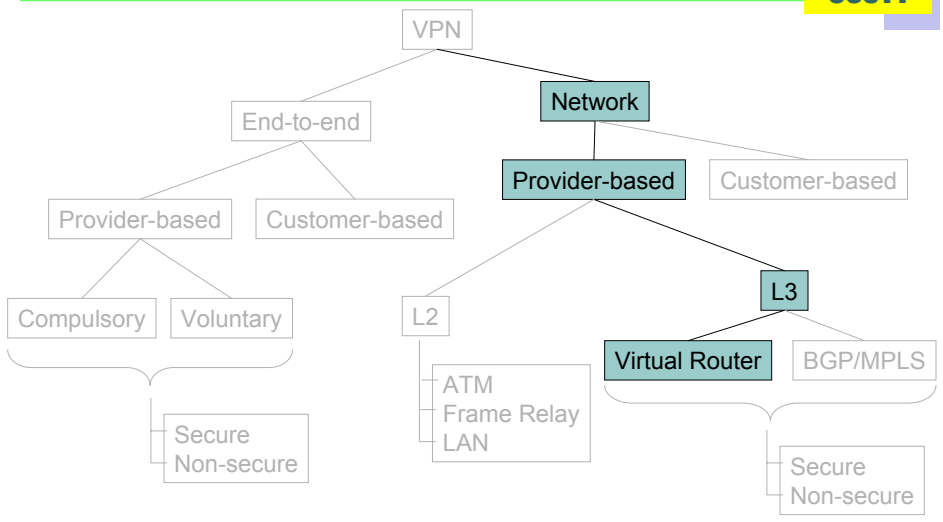
How BGP/MPLS VPNs work

CS514

- BGP updates normally carry a set of IP prefixes in the routing path
- With MPLS VPN, they carry a VPN identifier, and an MPLS tag
  - VPN identifier distinguishes overlapping address
  - MPLS tag says how to encapsulate customer's IP over MPLS
- Within MPLS, the tag both routes the packet and identifies the customer
- Tunnels are typically not secure
  - Customer assumes provider links are physically secure

Virtual Router based L3 VPNs

CS514



Virtual Router based L3 VPNs

CS514

- BGP/MPLS gave Cisco a huge advantage
  - Because Cisco was the BGP and MPLS expert
- Competitors' counter argument:
  - No need to couple routing technology with tunneling technology…they are separate issues
  - Simpler to use virtual routers

What is a virtual router (VR)?

CS514

- Separate logical router within a single physical router
  - Runs its own routing algorithm
  - Has its own FIB (Forwarding Information Base)
- Basic idea: Incoming tunnel identifies which VR is intended
  - If GRE, then GRE key field
  - If IPsec, then IPsec SPI field
  - If L2TP, then L2TP key field
- This is how overlapping addresses are distinguished

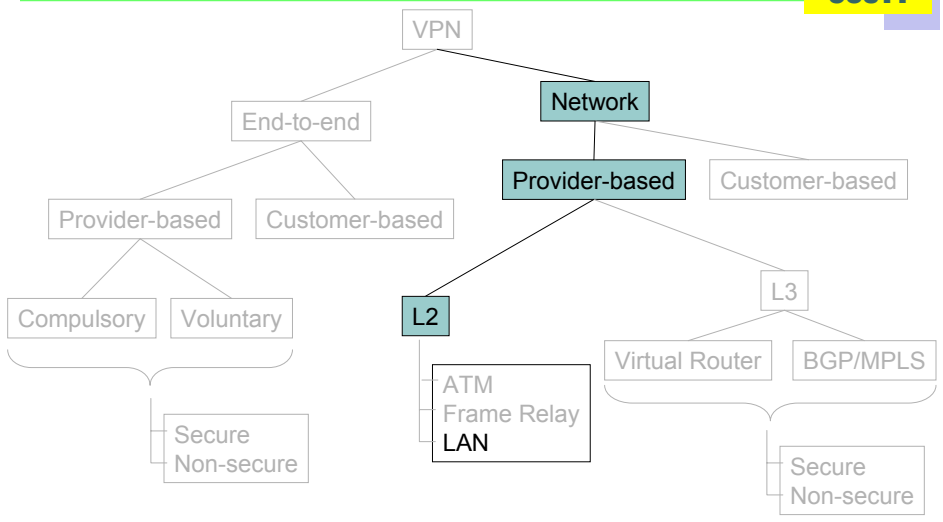
VR approach has discovery issues

CS514

- No standard way to configure tunnels and discover which PEs attach to which customers
  - All manually configured (via management system)
- Various proposals exist
  - Via BGP, OSPF, DNS, an LDAP database, and even IP multicast

Layer 2 LAN VPNs

CS514



Layer 2 LAN VPNs

CS514

- Current IETF project
- Model is for PE to look like LAN to CE
- CE broadcast over LAN reaches only other CEs of the same customer
  - Thus customer can run OSPF over LAN in standard way
  - Supports multicast
  - Multi-protocol
- Probably uses VLAN (Virtual LAN) tags to distinguish customers
- Advantages over FR and ATM are:
  - Ethernet is more common interface
  - Supports broadcast/multicast