# Optimizing Networks for NASPI

Scott Pelton, CISSP
National Director
AT&T Enterprise Network Architecture Center

# Agenda

- Introduction & Definition
  - OSI Model
  - Point to Point vs. Any to Any
  - Public vs. Private
- AT&T Engineered Networks
  - Core Backbone Description
  - Security, Integrity, Reliability, Availability
- Virtual Private Networks (VPN)
  - Public: SSL, IPSec, and others
  - Private: MPLS
  - Options and Connectivity

# Introduction & Definition

# OSI Model

| | Data unit | Layer | Function |
|---|---|---|---|
| Host layers | Data | 7. Application | Network process to application |
| | | 6. Presentation | Data representation and encryption |
| | | 5. Session | Interhost communication |
| | Segment | 4. Transport | End-to-end connections and reliability (TCP) |
| Media layers | Packet/Datagram | 3. Network | Path determination and logical addressing (IP) |
| | Frame | 2. Data link | Physical addressing (MAC & LLC) |
| | Bit | 1. Physical | Media, signal and binary transmission |

OSI Model courtesy of Wikipedia
http://en.wikipedia.org/wiki/OSI_model

# Characteristics of Networks

## Layer 2 Network

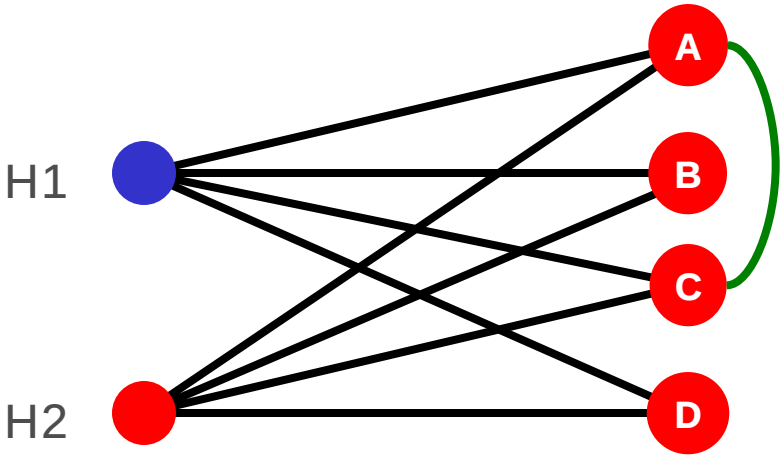
- OSI Data Link Layer
- Point to Point; Circuit Based
- Secure
- Mesh becomes expensive and difficult $\frac{n(n-1)}{2}$
- Dial, X.25, SNA, Frame Relay, ATM, etc.
- Hub and Spoke most common
- MAC & LLC Addressing (Hardware)

## Layer 3 Network

- OSI Network Layer
- Any to Any data paths
- Private is secure; Public is not
- Packet Switched – pre-defined routes
- Mesh is inherent
- Internet, MPLS Networks
- Private defined networks common; yet public Internet most ubiquitous
- IP Routing (Packet Header)

# Point to Point vs. MPLS Network View

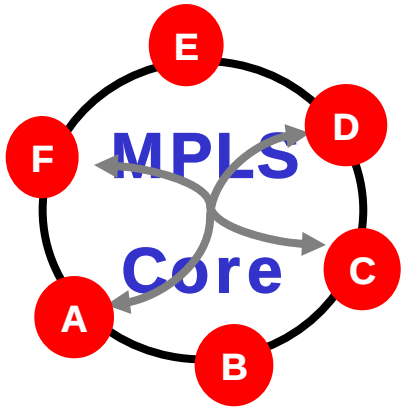

Simple Point to Point




Typical Point to Point

Hub and Spoke

(with second hub and partial MESH)




MPLS

Customer Defined Network

(Any to Any)

*Built in Disaster Recovery*

# MPLS Basics

- Any to Any connectivity within customer defined network
- **M**ulti**P**rotocol **L**abel **S**witching is a hybrid L2 and L3 protocol
- Independent customer networks predefined via Virtual Routing and Forwarding (VRF) tables
- Uses MPLS labels to traverse authorized path (VRF)
- Actual path can be dynamically determined depending upon network and traffic conditions (within the VRF)
- AT&T uses MPLS within our Core Backbone
- AT&T is a world-leader in providing private customer MPLS networks
- MPLS offers Class of Service (assigning priorities to traffic types)
- Private MPLS networks have same security characteristics as L2 networks

# Public vs. Private

## PUBLIC (UNTrusted)

- Internet is a Public Network
  - Publicly Accessible
  - Network of Networks
  - Inherently INSECURE
    - No universal safeguards in place
    - Variable and Unknown data path
    - Packet Headers can be spoofed and re-directed

## PRIVATE (Trusted)

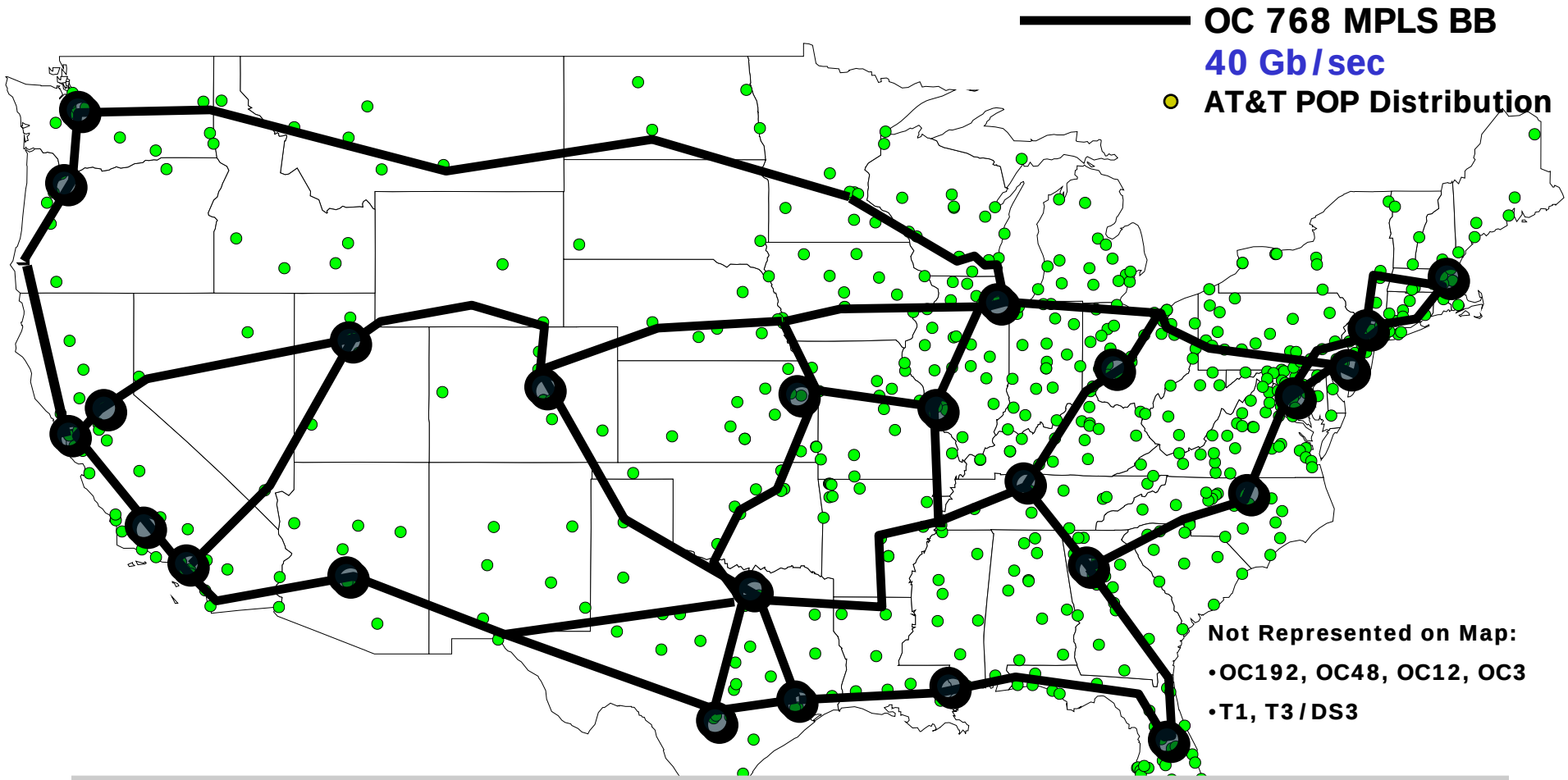
- Private Networks do not allow external access except through controlled measures
  - Access Control and Authentication:  Token, SSL, IPSec, etc.
- Point to Point (L2 Networks) are inherently secure
- MPLS Networks using VRF are inherently PRIVATE

# Value of MPLS

- Any to any connectivity within a VPN, allowing enterprise level security.
- Highly scalable .
- Level of security equivalent to Frame Relay or ATM through logical partitioning of traffic and routing information.
- Standards compliant, RFC 2547.
- Transition from frame-relay network technologies.
- Failure recovery is simple, leading to increased network stability
- Quality of service mechanisms allow one solution for voice, video and data
- Easy to manage, no virtual circuit provisioning required
- Can use private addresses within VPN
- Scaleable full mesh connectivity with single connection per location, leading to lower costs and more flexibility

# AT&T Engineered Networks

# OC768 Capable MPLS Core Network



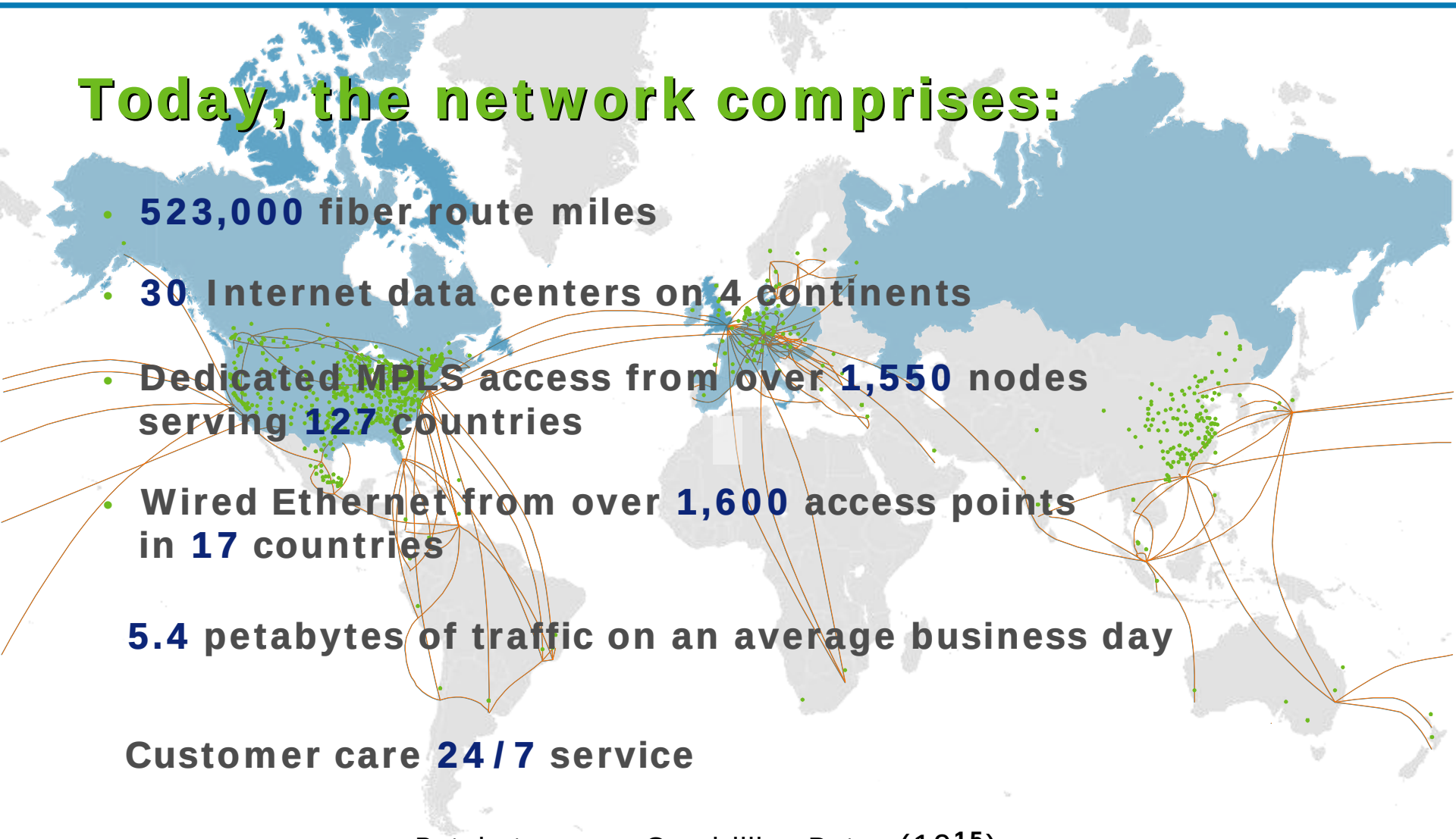

**There are many kinds of POPs (AT&T Point of Presence offices)**

**For T1 service, there are greater than 600 POPs nationwide (CONUS)**



at&t

# AT&T Global Network Leadership



## Today, the network comprises:

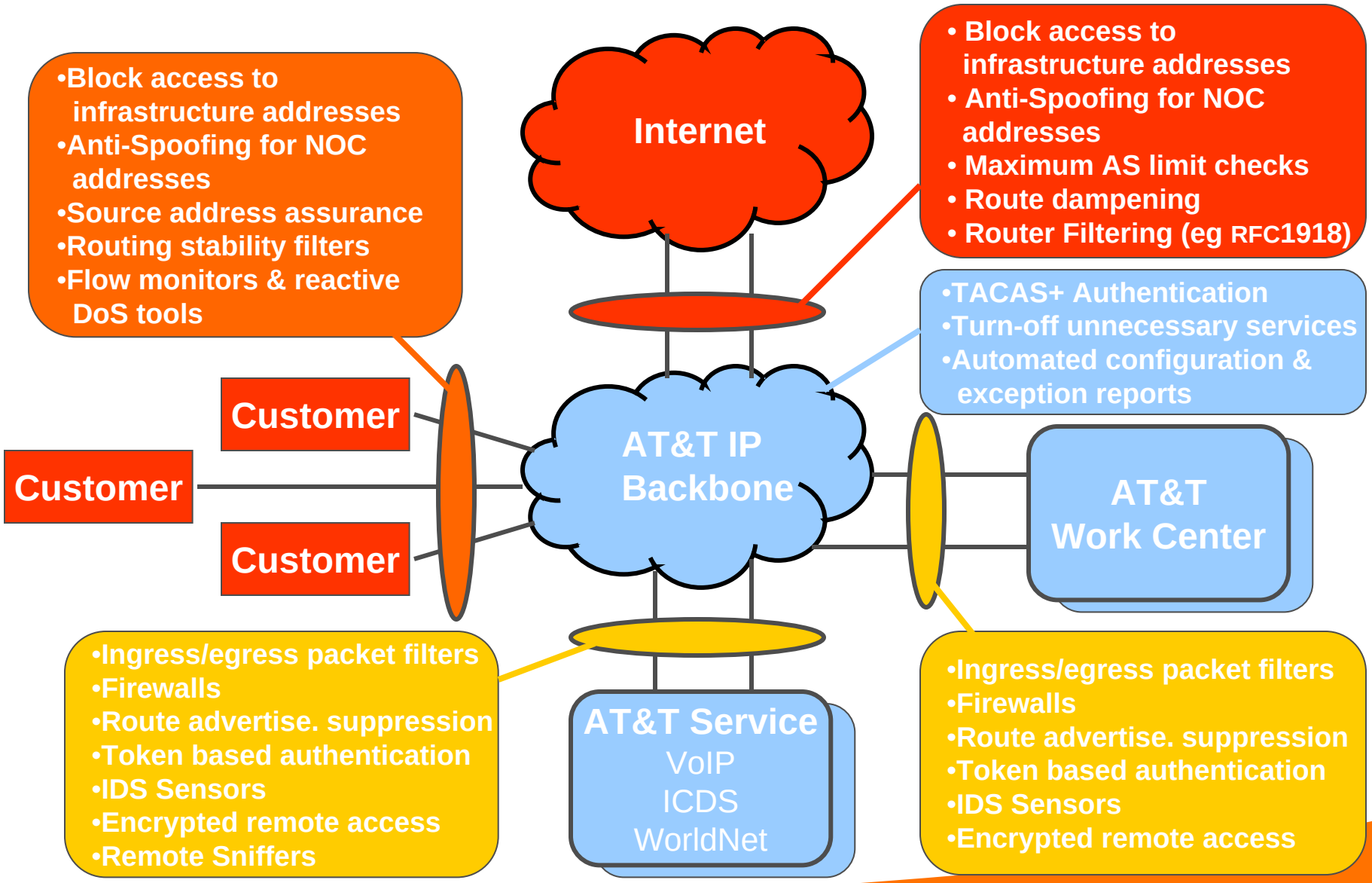
- **523,000** fiber route miles
- **30** Internet data centers on 4 continents
- Dedicated MPLS access from over **1,550** nodes serving **127** countries
- Wired Ethernet from over **1,600** access points in **17** countries

**5.4** petabytes of traffic on an average business day

Customer care **24/7** service

Petabyte = one Quadrillion Bytes ($10^{15}$)

# How AT&T Secures its MPLS Network and Global Network Backbone

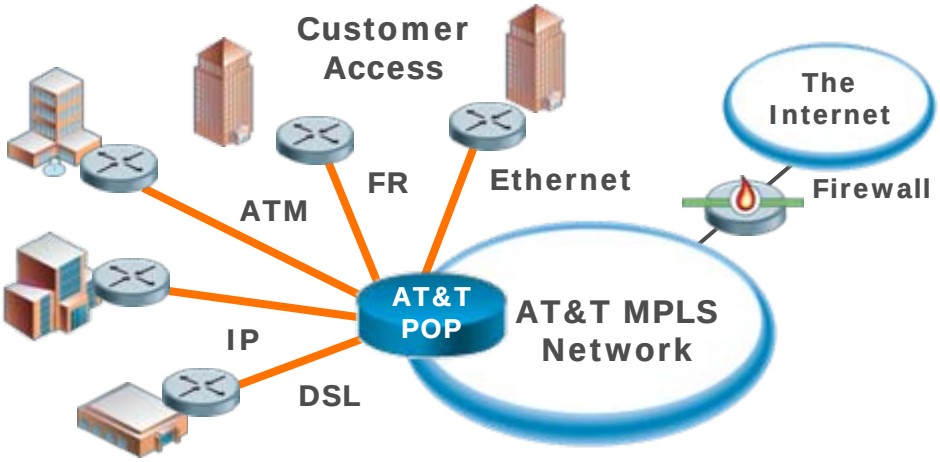


# AT&T VPN Service

## Customer Network

### AT&T VPN

- Network-Based IP VPN Service enabled by **Multiprotocol Label Switching (MPLS)**
- **Application awareness** supported by Class of Service (CoS)




## Features

- **MPLS inherent security**
- Variety of **access options**
- **Global** availability
  **Diversity Options** -FR & ATM MPLS ports (US availability)
- **Unilink**
- **Multicast** U.S. availability; MOW Controlled Introduction
- **Multi-link Point-to-Point Protocol (MLPPP)** (US availability)
- **Service Level Agreements**
- **Award-winning AT&T BusinessDirect™ portal**

## Client Benefits

- **Application awareness**
- **Scalability**
- Agile, reliable, flexible **any-to-any connectivity**
- **Easy access** to **reporting / tools**
- **Industry-leading Service Level Agreements**
- **Investment Protection**
- **Meshed network** with **Class of Service**
- Built-in **Disaster Recovery**

**Security, Integrity, Reliability, Availability**



at&t

# Virtual Private Networks

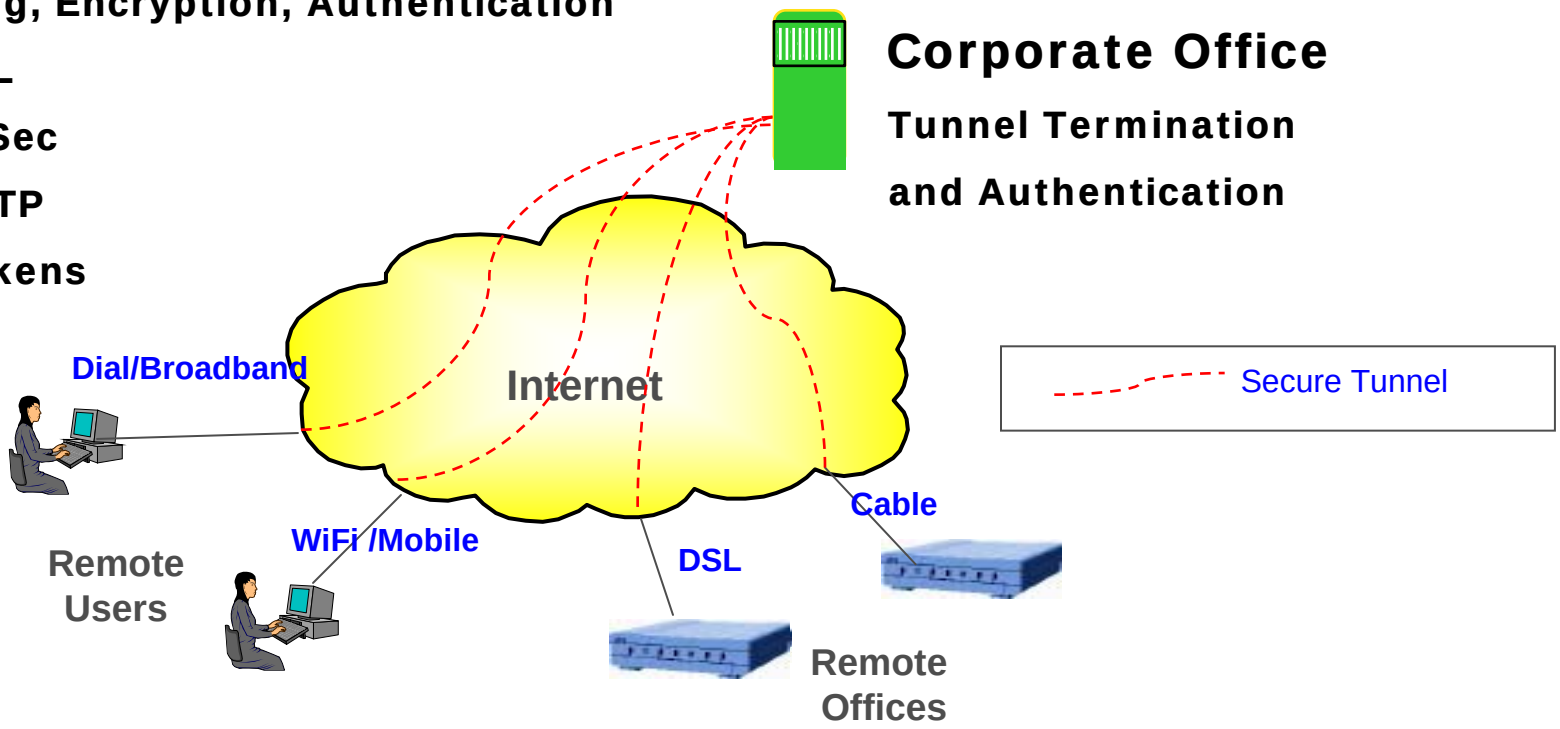
# VPN over Internet Architecture

## Premise Based VPN

### Technologies Employed at Remote Locations and Head Office

**Tunneling, Encryption, Authentication**

- **SSL**
- **IPSec**
- **PPTP**
- **Tokens**




**Internet (Untrusted, Public) + VPN Technologies = Secure Network**

Typically Point to Point Tunnel

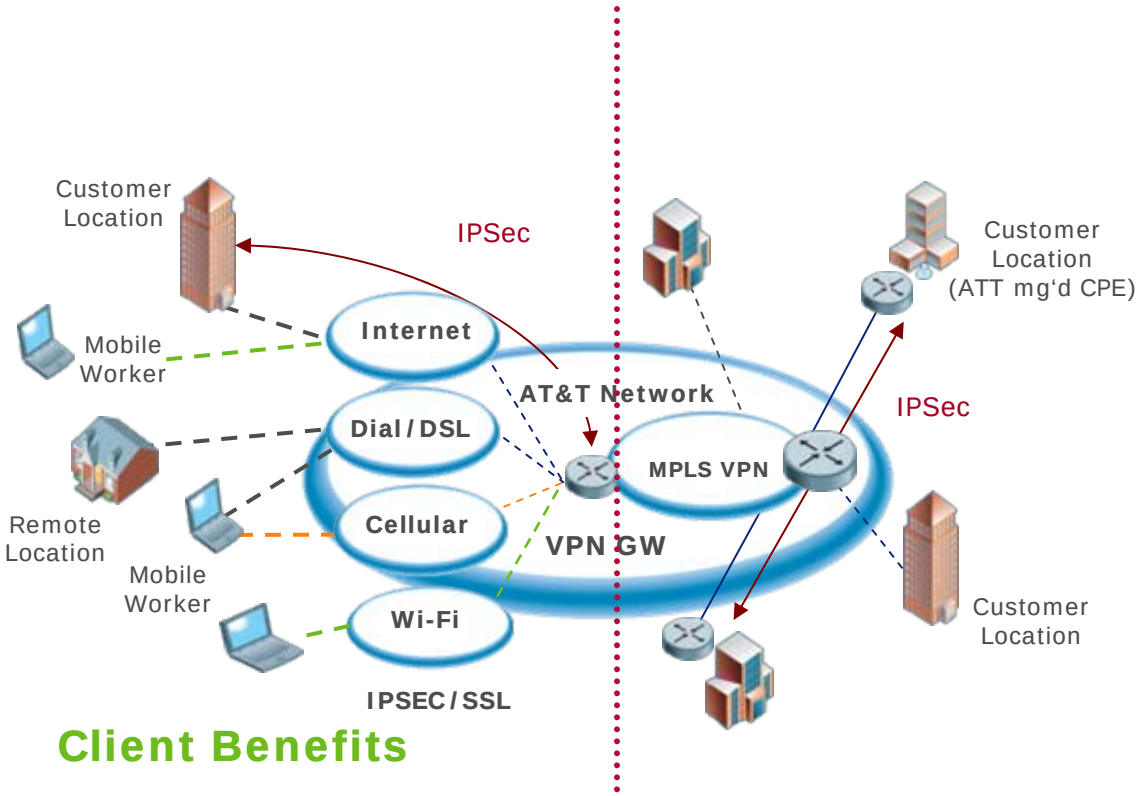
# AT&T MPLS VPN
## Network Based VPN

### AT&T VPN

- Multiprotocol Label Switching (MPLS)
- Any to Any Connectivity
- Application awareness supported by Class of Service (CoS)

### Features

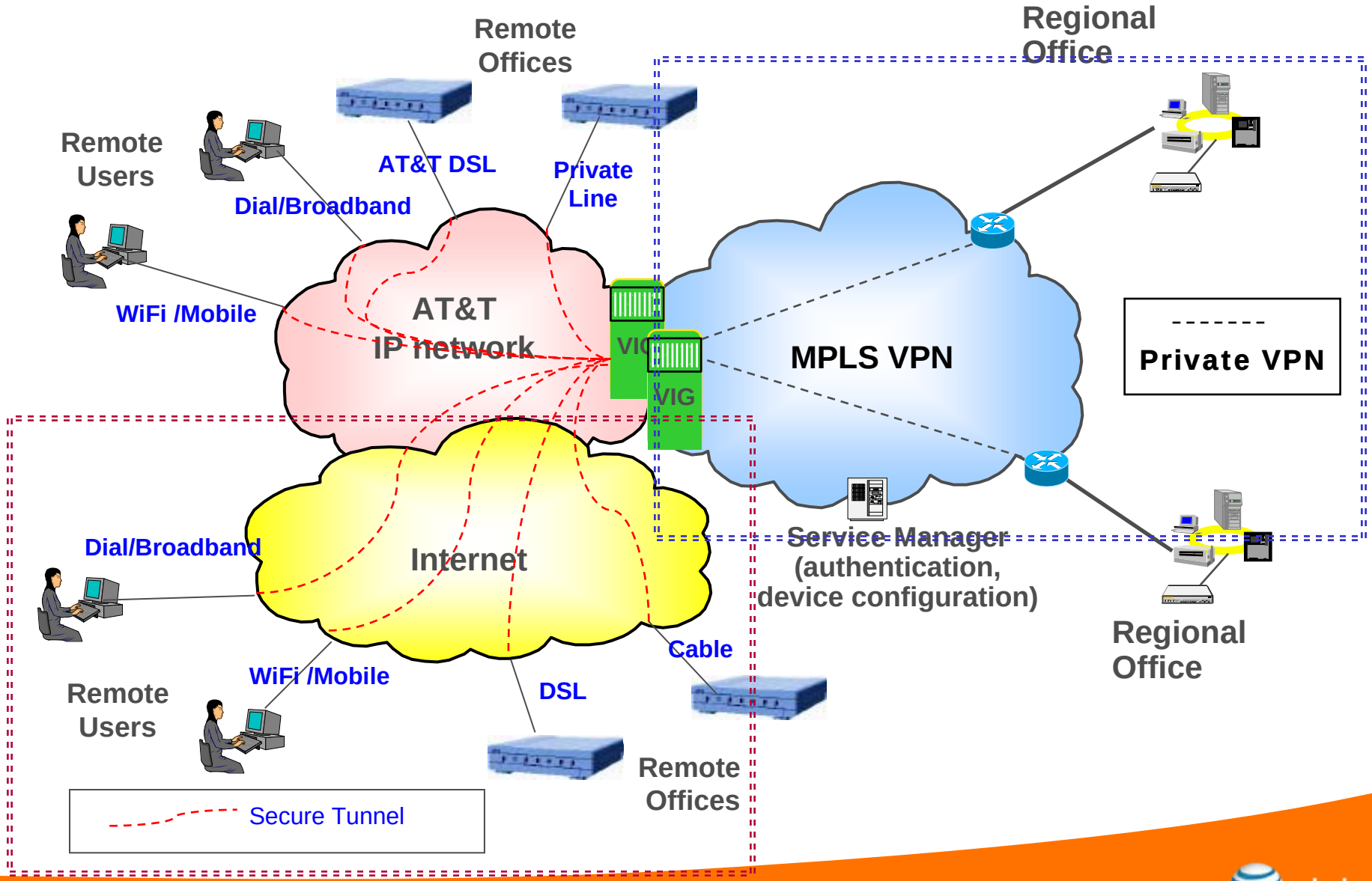
- MPLS inherent security capabilities
- Variety of access options
- Domestic and Global availability
- Feature rich services
- Service Level Agreements
- Integration of wireline and wireless
- Award-winning AT&T BusinessDirect® portal




### Client Benefits

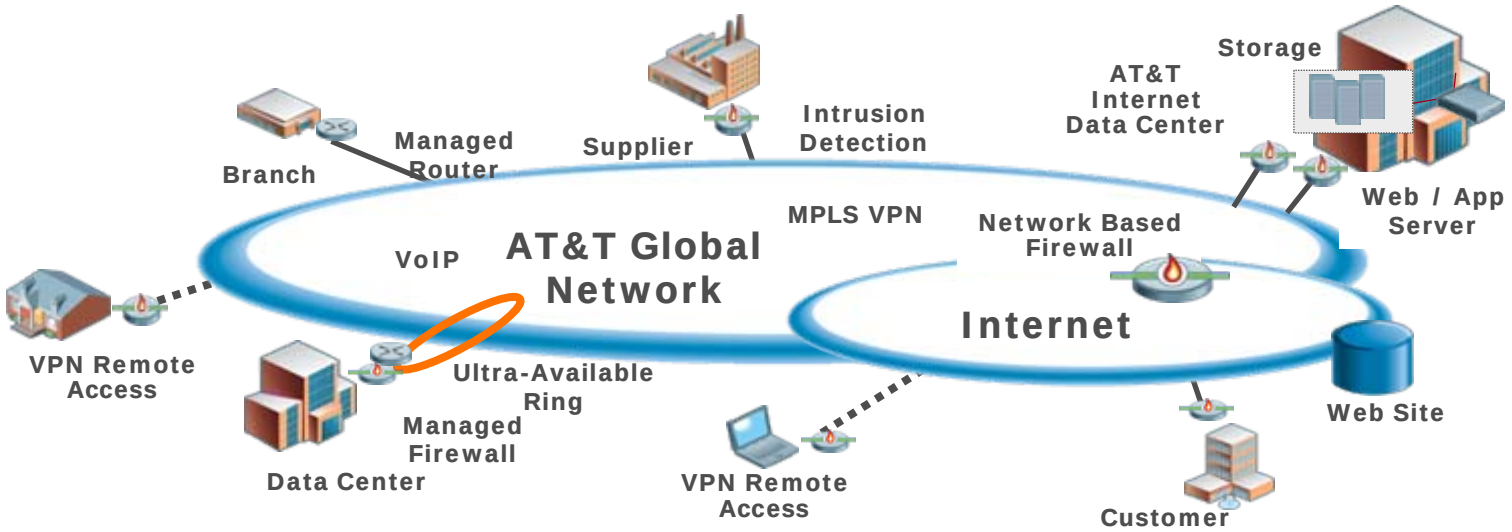
- Application awareness
- Scalability
- Agile, reliable, flexible, any-to-any connectivity
- Easy to access reporting / tools
- Industry-leading Service Level Agreements
- Investment Protection
- Meshed network with Class of Service
- Built-in Disaster Recovery

# AT&T Integrated Remote Access to Private Network (ANIRA)



# AT&T VPN – The Added Value

## Designing Complete Solutions




### Application Value Adds

- Voice over IP / LAN Telephony
- Content Hosting
- Storage Management
- Remote Access
- AT&T VPN Tunneling Service (AVTS)
- Network Based Video Bridging
- WAN Optimization – 1Q08

### Security Value Adds

- Managed Firewall
- Managed Authentication
- Anti-Virus Scanning
- InterNet Protect (Intrusion Detection)
- Private Intranet Protect

### Transport / Access Value Adds

- Private Line
- Frame Relay / ATM
- AT&T Network-based IPVPN Remote Access (ANIRA)

# Delivering Differentiated Networking Value

## Enterprise Networking Solutions

### Performance

- Consistent global architecture, seamlessly integrated
- Unsurpassed application performance around the world
- Industry leading Service Level Agreements for VPN's
  - Site Availability / TTR
  - Latency/Packet Delivery/Jitter
  - On-Time Provisioning
- Always-on infrastructure and recovery capabilities
- In-country / in-language end-user support

### Agility

- Integrate wireline and wireless solutions
- Any-to-any connectivity regardless of access type, location or speed
- Traffic prioritization with ability to set performance at transaction level
- AT&T Global Network Client enabling intelligent, integrated access selection
- Leading network convergence to IP VPN and IP applications

### Control

- Global Network Operations Center network monitoring 24/7
- Industry leading, award winning AT&T BusinessDirect® portal
- Global Network Client with end-user control
- Enterprise determines extent of access for end-users
- Manage costs as well as existing investments
- Service level preferences (congestion, latency, security); network manages administration

### Security

- Network-based, technology inherent protection
- Optional Personal Firewall
- Encrypted site to site connectivity
- Intrusion detection as network safeguard
- Dedicated connectivity between AT&T and customer data center
- Infrastructure helps ensure confidentiality and integrity of communications
- Device level, application and end-to-end security service best practices

# Thank You

## Questions ?