Deploying Multiservice Networks, VPNs, and DSL in Small Enterprise Branch Offices and Small/Medium Businesses

Session 2308
SMB and Small Branch Offices—Trends and Requirements

- Market and Technology Trends
- Key Applications
- Design/Implementation Considerations
- Cisco SMB and Small Branch Solutions
Agenda

- Market and Technology Trends
- Key Applications
- Design/Implementation Considerations
- Cisco SMB and Small Branch Solutions

Why Multiservice?

- Allows network convergence
  - Lower network capital costs
  - Packet infrastructure cost efficiencies
  - Lower network transport costs
  - Compression economies, nonconsequential busy hours, and single network (data and voice) volume economies
- Enable new services
  - Interactive call centers, enhanced fax services, video calls, expand into new markets, and voice messaging
Toll Bypass

Small Branch Office
- Phone
- Fax
- KTS/PBX
- Cisco 1750
- IP Phone

Branch Office
- PSTN
- PBX
- Cisco 2600/3600
- Gatekeeper
- MCM
- Intranet
- Frame Relay
- ISDN
- PSTN

Headquarters
- PBX
- Cisco 3660/7200
- Cisco Voice Manager (CVM)

Off Premise Extensions (OPX)

Small Branch Office
- Cisco 1750
- PSTN
- WAN (VoIP or VoFR) with QoS

Headquarters
- PBX
- Cisco 3640

Uses Connection Trunk Feature to Deliver Analog PBX Services to Remote Phones
Why VPNs?

- Allows connectivity for remote locations and mobile users at a lower cost than traditional WAN services
- Offers flexibility and security in deploying networks with varying access methods
- Easy migration to newer technologies

E-VPN Applications

**Intranet VPN**
- Low Cost, Tunneled Connections with Rich VPN Services, Like IPSec Encryption and QoS to Ensure Reliable Throughput
- Cost Savings over Frame Relay and Leased Lines

**Extranet VPN**
- Extends WANs to Business Partners
- Safe Layer 3 Security

**Remote Access VPN**
- Secure, Scalable, Encrypted Tunnels across a Public Network, Client Software
- Cost Savings over Toll-Free # Expenditures
Why Broadband Services?

- Better price/bandwidth vs. traditional access services
- Facilitates using existing copper for data and voice traffic
- For service providers, conserves copper facilities
- Allows deployment of enhanced services (multiservice, VPNs, etc.)

Applications Will Drive DSL

- DSL is an enabling technology for high-bandwidth (always on) applications
- VoATM (AAL2) will be a key application for DSL deployment
- AAL2: draft recommendation (ITU-T) for sending small packets (e.g., voice) over an ATM network with small delay
  - Supports muxing multiple connections into a single cell
  - Supports muxing variable length packets (important for variable bit-rate coders and silence suppression)
End-to-End DSL Network Architecture

- Local Voice Services
- Managed Voice and Data VPNs
- Add’l Lines On-demand
- Private Line Replacement
- Video Conferencing
- Video-on-Demand
- High-speed Internet Access

Agenda

- Market and Technology Trends
- Key Application Enablers
- Design/Implementation Considerations
- Cisco SMB and Small Branch Solutions
Multiservice Network Design Considerations

- Layer 2, Layer 3 transport choice
- Voice quality and bandwidth trade-off (codec selection vs. bandwidth)
- Quality of service
- Scalability (gatekeeper and dial plan)
- Manageability and monitoring (CVM)

VoIP/VoFR/VoATM—Which One?

- Cisco is technology agnostic: voice over IP, FR, or ATM, depending on customer requirements
- Customers with router-based backbones will gravitate to VoIP solutions
- VoIP enables interoperability with I-Phone, H.323, and other LAN-based telephony applications
- Customers with switched backbones may prefer voice over Frame Relay, VoATM solutions
- Cisco is providing end-to-end solutions for many different applications
- Analysts predict VoIP will have the most long-term growth opportunity
# Multiservice Challenges and Solutions

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prioritization</td>
<td>QoS, IP Precedence</td>
</tr>
<tr>
<td>Echo</td>
<td>Standards-Based Echo Cancellation G.165</td>
</tr>
<tr>
<td>Packet Loss</td>
<td>Autofill in Algorithm</td>
</tr>
<tr>
<td>Delay</td>
<td>Use of Real-Time Protocol, Queuing, Algorithms, Prioritizations, DSPs</td>
</tr>
<tr>
<td>Jitter</td>
<td>Dynamic Buffer Allocation</td>
</tr>
<tr>
<td>Bandwidth Utilization</td>
<td>Use of Standards-Based Voice Compression, Fragmentation, and QoS</td>
</tr>
</tbody>
</table>

## Payload Bandwidth Requirements for Various Codecs

<table>
<thead>
<tr>
<th>Encoding/Compression</th>
<th>Resulting Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>G.711 PCM A-Law/u-Law</td>
<td>64 kbps (DS0)</td>
</tr>
<tr>
<td>G.726 ADPCM</td>
<td>16, 24, 32, 40 kbps</td>
</tr>
<tr>
<td>G.727 E-ADPCM</td>
<td>16, 24, 32, 40 kbps</td>
</tr>
<tr>
<td>G.729 CS-ACELP</td>
<td>8 kbps</td>
</tr>
<tr>
<td>G.728 LD-CELP</td>
<td>16 kbps</td>
</tr>
<tr>
<td>G.723.1 CELP</td>
<td>6.3/5.3 kbps</td>
</tr>
</tbody>
</table>
VoIP Packet Format

Payload Size, PPS and BPS Vendor Implementation Specific; for Example:

Not Including Link Layer Header or CRTP

<table>
<thead>
<tr>
<th>Media</th>
<th>Link Layer Header Size</th>
<th>Bit Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet</td>
<td>14 Bytes</td>
<td>29.6 kbps</td>
</tr>
<tr>
<td>PPP</td>
<td>6 Bytes</td>
<td>26.4 kbps</td>
</tr>
<tr>
<td>Frame Relay</td>
<td>4 Bytes</td>
<td>25.6 kbps</td>
</tr>
<tr>
<td>ATM</td>
<td>5 Bytes Per Cell</td>
<td>42.4 kbps</td>
</tr>
</tbody>
</table>

Note—For ATM a Single 60 Byte Packet Requires Two 53 Byte ATM Cells

Various Link Layer Header Sizes

Varying Bit Rates Per Media

Example—G.729 with 60 Byte Packet (Voice and IP Header) at 50 pps (No RTP Header Compression)
Effect of QoS on Voice Quality

Source: Cisco Labs

Large Packets Freeze Out Voice

- Large packets can cause playback buffer under run; resulting in slight voice degradation
- Jitter or playback buffer can accommodate some delay/delay variation
PQ-CBWFQ

Class-map data
match input-interface Ethernet0/0

Class-map voice
match access-group 101

Policy-map WAN
Class voice
priority 80

Class data
bandwidth 16
random-detect

Class class-default
fair-queue
random-detect

interface Serial0/1
ip address 10.1.1.1 255.255.255.0
bandwidth 128
no ip directed-broadcast
service-policy output WAN

access-list 101 permit ip any any precedence critical

PQ Class Based WFQ

Class-map voice = 80 kbps

Class-map data = 16 kbps

Class-map class-default

Any Packet with IP Precedence = 5 Gets Assigned to a Class that Will Get a Minimum of 80 kbps on a 128 kbps Circuit

Header Compression: CRTP

- CRTP—Compressed Real-Time Protocol
- RFC 2508
- G.729: 20 ms @ 8 kbps yields 20 byte payload
- 40 bytes per packet: IP header 20; UDP header 8; RTP header 12
- Header compression 40 bytes to 2-4 much of the time
- Hop-by-hop on slow links
Link Efficiency—Send Fewer Packets

- **VAD**
  
  B versions of G.729 contain a built-in IETF VAD algorithm; no need to configure VAD
  
  Rule-of-thumb: 30–35% reduction in BW—a more valid assumption for larger pipes (T1 and above)
  
  Depends on application (e.g. music-on-hold makes VAD 0%)

- **Variable payload size**
  
  Specify # samples per packet
  
  Usability depends on the delay budget of the network
  
  Values > default: decreases bandwidth, and increases delay
  
  Values < default: increases bandwidth, and decreases delay

Fragmentation Recommendations

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>10 ms</th>
<th>20 ms</th>
<th>30 ms</th>
<th>40 ms</th>
<th>50 ms</th>
<th>100 ms</th>
<th>200 ms</th>
</tr>
</thead>
<tbody>
<tr>
<td>56 kbps</td>
<td>70 Bytes</td>
<td>140 Bytes</td>
<td>210 Bytes</td>
<td>280 Bytes</td>
<td>350 Bytes</td>
<td>700 Bytes</td>
<td>1,400 Bytes</td>
</tr>
<tr>
<td>64 kbps</td>
<td>80 Bytes</td>
<td>160 Bytes</td>
<td>240 Bytes</td>
<td>320 Bytes</td>
<td>400 Bytes</td>
<td>800 Bytes</td>
<td>1,600 Bytes</td>
</tr>
<tr>
<td>128 kbps</td>
<td>160 Bytes</td>
<td>320 Bytes</td>
<td>480 Bytes</td>
<td>640 Bytes</td>
<td>800 Bytes</td>
<td>1,600 Bytes</td>
<td>3,200 Bytes</td>
</tr>
<tr>
<td>256 kbps</td>
<td>320 Bytes</td>
<td>640 Bytes</td>
<td>960 Bytes</td>
<td>1,280 Bytes</td>
<td>1,600 Bytes</td>
<td>3,200 Bytes</td>
<td>6,400 Bytes</td>
</tr>
<tr>
<td>512 kbps</td>
<td>640 Bytes</td>
<td>1,280 Bytes</td>
<td>1,920 Bytes</td>
<td>2,560 Bytes</td>
<td>3,200 Bytes</td>
<td>6,400 Bytes</td>
<td>12,800 Bytes</td>
</tr>
<tr>
<td>768 kbps</td>
<td>1,000 Bytes</td>
<td>2,000 Bytes</td>
<td>3,000 Bytes</td>
<td>4,000 Bytes</td>
<td>5,000 Bytes</td>
<td>10,000 Bytes</td>
<td>20,000 Bytes</td>
</tr>
<tr>
<td>1,536 kbps</td>
<td>2,000 Bytes</td>
<td>4,000 Bytes</td>
<td>6,000 Bytes</td>
<td>8,000 Bytes</td>
<td>10,000 Bytes</td>
<td>20,000 Bytes</td>
<td>40,000 Bytes</td>
</tr>
</tbody>
</table>

**Recommendation for Voice**

Packet Serialization Delay

Fragmentation is Not Necessary above T1 (1.5M)
Traffic Shaping Overview

- **VoIP-over-serial:**
  Needs no traffic shaping
  BW is guaranteed at line speed
- **VoIPovFR and VoFR:**
  Use FRTS—applicable per VC
  GTS is applicable only per interface
  Set min-CIR equal to voice bandwidth and a little overhead to ensure good voice quality under WAN-congestion situations
  On PVC carrying voice, shape strictly to CIR—don’t burst
- **VoATM:**
  Use ATM traffic shaping

VoIP Low-Speed Link (<768 Kbps) Challenges and Solutions

<table>
<thead>
<tr>
<th>Challenge</th>
<th>Cisco Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Congestion</td>
<td>Intelligent Queuing</td>
</tr>
<tr>
<td>Delay and Delay Jitter</td>
<td>PQ/CBWFQ, IP Precedence, RSVP, Priority Queuing</td>
</tr>
<tr>
<td>Packet Residency</td>
<td>Interleaving</td>
</tr>
<tr>
<td>Slow Link Freeze-out by Large Packets</td>
<td>FRF.12, MLPPP, IP MTU Size Reduction, Faster Link</td>
</tr>
<tr>
<td>Bandwidth Consumption</td>
<td>Compression</td>
</tr>
<tr>
<td>Header Size on Low Bandwidth Links</td>
<td>Codecs, RTP Header Compression, Voice Activity Detection</td>
</tr>
<tr>
<td>WAN</td>
<td>Traffic Management</td>
</tr>
<tr>
<td>Over Subcription, Bursting</td>
<td>Router Traffic Shaping to CIR, High-Priority PVC, Data Discard Eligibility</td>
</tr>
</tbody>
</table>
Gateway Initiated Calls—H.323 Gatekeeper

- Defined by H.323 (used in VoIP)
- Gateways auto register with gatekeeper
- Gateways initiate calls but do not know about other gateways
- Telephony E.164-style addresses mapped to IP addresses by gatekeeper
- H.323 gatekeepers allow scaling

H.323 Without RAS

- VoIP dial peer points directly to the destination gateway’s IP address
- Scaling to large networks becomes administratively burdensome
**H.323 With RAS**

**Registration, Admission, and Status**

Address Translation: Every Gateway Needs to know only about the Gatekeeper, not about all other Gateways

- **Gatekeeper**
- **Gateway A**
- **Gateway B**

**IP QoS**

**Network**

**H.225 (Q.931) Call Setup (TCP)**

**RTP (UDP)**

**H.245 Call Control (TCP)**

---

**RAS Configuration**

**Gatekeeper 1**

526-1111

- `zone local GK-1 cisco.com 10.1.5.1`
- `zone remote GK-2 cisco.com 133.10.20.4 1719`

**Gateway 1**

10.1.5.2

- `network-peer`
- `dial-peer voice 100 voip destination-pattern 526... session target ras`

**Gateway Interface e0**

- `ip address 10.1.5.2 255.255.0.0`
- `h323-gateway voip interface`
- `h323-gateway voip id GK-1 ipaddr 10.1.5.1 1719`
- `h323-gateway voip h323-id GW-1@cisco.com`

**Gateway 2**

10.1.5.4

- `network-peer`
- `dial-peer voice 200 voip destination-pattern 853... session target ras`

**Gateway Interface e0**

- `ip address 10.1.5.4 255.255.0.0`
- `h323-gateway voip interface`
- `h323-gateway voip id GK-2 ipaddr 10.1.5.1 1719`
- `h323-gateway voip h323-id GW-2@cisco.com`
**VPNs—Who Does What**

**Enterprise Managed**
- Service Provider provides basic VPN connectivity
- Enterprise manages QoS, security, SLA, and configuration of VPN functions

**Service Provider Managed**
- Service Provider provides turnkey VPN
- Enterprise outsources design, provisioning and management
- Enterprise controls security

---

**Elements of VPNs**

- **Management**
- **Provisioning**
- **Tunneling**
- **Security**
- **QoS**
Data Privacy Services

Separate Data Tunneling
- IPSec
- GRE
- L2TP
- L2F

Increase Protection Encryption
- IPSec
- DES, 3 DES

Prevent Tampering Integrity
- TCP Checksum
- AH in IPSec

Identify Source Authentication
- RSA
- PKI

Secure Integrated Software

• Enhanced, integrated security for Cisco IOS® platforms

  Full-featured firewall (CBAC)
  Active in-line intrusion detection
  Authentication proxy
  Supports NAT, IPSec VPN
  Secure remote administration

• Strong security at low cost
• Leverages investment in Cisco infrastructure
What Is Context-Based Access Control (CBAC)?

- Tracks state and context of network connections to secure traffic flow
- Inspects data entering or leaving router
- Allows connections to be established by temporarily opening ports based on payload inspection
- Return packets authorized for particular connection only via temporary ACL

CBAC: How Does It Work?

![Diagram showing how CBAC works]

Cisco IOS Firewall Router

ISPs and Internet

CBAC Creates Dynamic ACLs to Allow Connections Initiated from Inside

ACL Blocks All Connections Initiated from Outside
How the Cisco IOS Firewall Feature Set Works

- Inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions.
- Filters TCP and UDP packets based on application-layer protocol session information in addition to network layer and transport layer information.
- State information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions.

CBAC uses timeouts and thresholds to determine how long to manage state information for a session.

Protection against DoS attacks:
CBAC measures both the total number of existing half-open sessions and the rate of session establishment attempts.

You can configure CBAC to inspect the following types of sessions:
- All TCP sessions, regardless of the application-layer protocol (sometimes called "single-channel" or "generic" TCP inspection).
- All UDP sessions, regardless of the application-layer protocol (sometimes called "single-channel" or "generic" UDP inspection).

CBAC can also be configured to inspect specific application-layer protocols:
- CU-SeeMe (White Pine version), FTP, H.323 (NetMeeting, ProShare), Java, UNIX R-commands, RealAudio, RPC, SMTP, SQL*Net, StreamWorks, TFTP, and VDOLive.
Monitoring CBAC

- CBAC provides syslog messages, console alert messages and audit trail messages
- The following types of error messages can be generated by CBAC:
  - Denial-of-service attack detection error messages
  - SMTP attack detection error message
  - Java blocking error message
  - FTP error messages
  - Audit trail error message

Configuring Cisco IOS Firewall

- Define inspection rule
  - `ip inspect name myfirewall ftp timeout 3600`
  - `ip inspect name myfirewall rcmd timeout 3600`
  - `ip inspect name myfirewall realaudio timeout 3600`
  - `ip inspect name myfirewall smtp timeout 3600`
  - `ip inspect name myfirewall udp timeout 30`
  - `ip inspect name myfirewall tftp timeout 60`
  - `ip inspect name myfirewall tcp timeout 3600`
• Apply the inspection rule to inbound traffic—in this case, at Ethernet 0

  interface Ethernet0
  ip address 172.10.20.1 255.255.255.0
  ip inspect myfirewall in

Management and Provisioning

• Generic configuration
• AAA
• Policy management
• Certificate authorities
Certificates

- Certificate Authority (CA) verifies identity
- CA signs digital certificate containing device’s public key
- Certificate equivalent to an ID card

Digital Certificate

- A Digital certificate contains:
  - Serial number of the certificate
  - Issuer algorithm information
  - Valid to/from date
  - User public key information
  - Signature of issuing authority

- Example:
  - 0000123
  - RSA, 3837829...
  - 1/1/93 to 12/31/98
  - Alice Smith, Acme Corp
  - RSA, 3813710...
  - Acme Corporation, Security Dept.
  - RSA, 2393702347...
Steps in Configuring IPSec

- After choosing either pre-shared key or CA, there are four components in setting up IPSec—
  Create extended ACL
  Create IPSec transform
  Create crypto map
  Apply crypto map to interface
Sample IPSec Configuration

hostname remote_1
ip host remote_2.ribupme.com 18.0.0.3
crypto isakmp policy 1
  authentication pre-share
group 2
  crypto isakmp key sharedkey hostname remote_2.ribupme.com
crypto ipsec transform-set settings esp-3des esp-sha-hmac
crypto map mapname 10 ipsec-isakmp
  set peer 20.0.0.3
  set transform-set settings
  match address 103
interface Serial0
  ip address 18.0.0.2 255.255.255.0
  crypto map mapname

!  access-list 103 permit ip 10.0.0.0 0.0.0.255 10.1.1.0 0.0.0.255

Agenda

- Market and Technology Trends
- Key Applications
- Design/Implementation Considerations
- Cisco SMB and Small Branch Solutions
Cisco 1720

- **Flexibility**
  - Auto-sensing 10/100 Fast Ethernet +
  - two WIC slots + AUX port
  - Supports any combination of current 2600 WICs

- **Investment protection**
  - Supports New World Services including VPNs, broadband...now or later
  - Cisco IOS technologies
    - Security, QoS, management, reliability/scalability
  - RISC processor for encryption performance
    - IPSec DES encryption performance: 512 Kbps for 256-byte packets
  - Future option for hardware-assisted encryption at T1/E1

- **Network device integration**
  - Router-firewall-encryption-VPN tunnel server-DSU/CSU-NT1

![Cisco 1720 Hardware](image)

---

Cisco 1720 Architecture

**Chassis**
- RISC Processor for Encryption Performance
- One Autosensing 10/100 Fast Ethernet
- Console and Auxiliary Ports up to 115 kbps
- Cisco Networked Office Stack Enclosure
- Two Modular Slots with Data Support
- VPN, DSL Ready

**Memory**
- Runs from DRAM
  - DRAM Onboard/Default: 16 MB
  - DRAM Max: 48 MB
  - Flash Onboard/Default: 4 MB
  - Flash Max: 16 MB

**Two WAN Interface Card Slots**
- Any Combination of WAN Interface Cards
- Over 25 WAN Interface Combinations
- Serial, ISDN BRI, and CSU/DSU Options
- Shared with Cisco 1600, 2600, 3600 Series

**Internal Expansion Slot**
- Hardware-Assisted Data Encryption up to T1/E1
Cisco 1750

- **Flexibility and investment protection**
  - Modular product with one VIC slot, two VIC/WIC slots
  - Auto-sensing 10/100 Ethernet with console and AUX ports
  - Support for diverse WAN and Voice interface types
  - Multiservice/VPN access now or later
  - Internal slot for optional hardware-assisted encryption card
- **Multiservice access**
  - Multiservice data/voice/fax/video integration
  - Cisco IOS technologies with QoS
  - Future broadband access
- **Network device integration**
  - Voice/data-router-firewall-encryption-VPN-DSU/CSU-NT1

---

Cisco 1750 Architecture

**Chassis**
- RISC processor for encryption performance
- One autosensing 10/100 Fast Ethernet
- Console and auxiliary ports up to 115 kbps
- 3 Modular slots with 1 voice and 2 voice/data
- DSL, Multiservice, VPN ready

**Memory**
- Runs from DRAM
- DRAM onboard/default: 16 MB
- DRAM max: 48 MB
- Flash onboard/default: 4 MB
- Flash max: 16 MB

**One Voice and Two Voice/WAN Interface Card Slots**
- Any combination of WAN interface cards
- Any combination of analog voice interface cards
- Over 25 WAN interface combinations
- Serial, ISDN BRI, and CSU/DSU options
- WICs/VICs leveraged across multiple Cisco access products

**Internal Expansion Slot**
- Hardware-assisted data encryption up to T1/E1, data compression
 Cisco 1700—Flexible Device Integration to Enable New World Services

**Broadband Access**
- ADSL in August

**Access Router**
- Multiprotocol routing
- Diverse WAN access methods
- Scalable routing protocols

**Data/Voice Integration**
- Toll bypass
- Cisco IOS with QoS features
- Phone/fax/KTS/PBX interoperability
- Bandwidth management

**Cisco 1750 Only**
- IPSec

**Dedicated VPN Devices**
- Encryption performance
- Dynamic firewall
- VPN tunneling
- Optional Integrated hardware encryption module

**Multiservice Voice/Data Integration**

**Small Branch Office**
- Phone
- KTS/PBX
- Fax
- Cisco 1750

**Branch Office**
- PSTN
- PBX
- Cisco 2600/3600

**Headquarters**
- Intranet
- Leased Line
- Frame Relay
- ISDN
- Leased Line Frame Relay
- ISDN
- Cisco 3660/7200
- MCM Gatekeeper
- Cisco Voice Manager (CVM)
VPN Access

- Branch to branch
- Remote user access
- Extranet
- Integrated single-vendor solution
  - Voice/data integration
  - Router-firewall-VPN tunnel
  - server-DSU/CSU-ISDN
  - NT1-hubs/switches
  - Single phone call for support
  - Easy to use and manage

Cisco 1700 Series: VPN Module

- Accelerates IPSec (3DES) up to full duplex T1/E1 serial
- Delivers up to 100 concurrent sessions
- Fits in expansion slot inside chassis
- 3DES or DES for data protection
- RSA and Diffie-Hellman for authentication
- SHA-1 or MD5 hashing algorithms for data integrity

Released in April 2000 (Cisco IOS 12.1(1)XC) List Price: $1,000
DSL Access

Small Branch Office

Cisco 1700

Cisco 6X00 (DSLAM)

ADSL

WAN

Headquarters

Cisco 3600

DSL Connectivity to SMB and Small Branch Office Customers

ADSL WIC Overview

- Fully-managed WIC available on Cisco 1700/2600/3600 platforms
  - FCS on Cisco 1700 August 2000, FCS on Cisco 2600/3600 Dec. 00/Jan. 01
- Enables communications of 8 MB downstream and 1 MB upstream
  - 500 kbps bi-directional with 3DES hardware encryption (Cisco 1700)
- Enables VoIP/DSL communications and VoATM (FCS+)
- Provides differentiated service levels for voice (AAL2), critical data, interactive multimedia, and videoconferencing applications
### ADSL WIC Features

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ATM Features</strong></td>
<td>• ATM AAL2 and AAL5&lt;br&gt;• PPP over ATM (IETF Version), RFC 1483 (Bridging and Routing), RFC 1577&lt;br&gt;• CBR, VBR-NRT, VBR-RT, UBR&lt;br&gt;• 50 PVS on WIC, 256 on 26/3600&lt;br&gt;• ATM Fault Management (OAM-F5 and ILMI)&lt;br&gt;• ATM UNI 3.1 PVC&lt;br&gt;• Per VC Traffic Shaping</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>SNMP, Telnet, ATM MIB, and Console Port</td>
</tr>
<tr>
<td><strong>Voice Features</strong></td>
<td>VoIP Features per Cisco 1700/2600/3600 Platform Including Fast-Switched cRTP, Fast-Switched MLPPP, and PQ/CBWFQ</td>
</tr>
</tbody>
</table>

### ADSL WIC Features (Cont.)

<table>
<thead>
<tr>
<th>Category</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ADSL Features</strong></td>
<td>• ANSI T1.413 Issue 2&lt;br&gt;• ITU G.992.1 (G.DMT)&lt;br&gt;• ITU G.992.2 (G.LITE)*</td>
</tr>
<tr>
<td><strong>Hardware Features</strong></td>
<td>• WIC form Factor&lt;br&gt;• LEDS: OK, Carrier Detect, and Loopback&lt;br&gt;• Alcatel MTC-20150 Chipset</td>
</tr>
<tr>
<td><strong>DSLAM Compatibility</strong></td>
<td>• Alcatel DMT 2 DSLAM&lt;br&gt;• Cisco 6130/6260 DSLAM with 4x ADI DMT 2 and 4x Flexi Line Cards</td>
</tr>
</tbody>
</table>

*As limited by chipset*
Cisco 1700 Series Applications
Today and Future

- Voice/Data Integration
- Managed Voice/VPN Services
- Secure Access for Small Business
- Distance Learning and Video-Conferencing
- Voice Applications
- High-Speed Internet Access with DSL

DSL CPE Market Segments
Cisco IOS = Business Class

- Residential Partners
- Entry Level
- Business Class SOHO/Telecommuter
- Small/Med Business/Small Branch
- Enterprise Branch

- Cisco 800
- Cisco 1700 with DSL WIC
- CBOS

- Differentiated Classes of Service
- Integrated Toll Quality Voice
- Business Class Security and VPN
- Mission-Critical Reliability and Manageability
Business DSL Defined

- E-commerce
- Videoconferencing
- Fax on demand
- Distance learning

- Voice
- Video
- VPN
- Managed services
- Differentiated classes of service

- QoS features
- Voice
- Security
- Reliability and manageability

End-Customer Requirements

Residential
- Plug and Play, Competitive Pricing

Small to Medium-Sized Business
- QoS, Voice/WAN
- Cost Reduction, Security, Reliability

Branch Office, Telecommuter
- Lower Voice/WAN Cost, Security, Efficient Use of Bandwidth
Cisco 827 Benefits

Power of Cisco IOS Technology for Small Offices and Telecommuters

• Benefits of business-class functionality
  - Differentiated classes of service
  - Integrated toll quality voice/data
  - Business-class security
  - Mission-critical reliability

• Reduced cost of operations
  - Cisco IOS manageability: proactive diagnostics, debug
  - Familiarity of Cisco IOS CLI

Cisco 827 ADSL Router

• Two models:
  - Cisco 827: 1E, 1ADSL
  - Cisco 827-4V: 1E, 1ADSL, 4Voice

• G.DMT today; G.Lite H2/CY ’00
  - Alcatel chipset

• Cisco IOS software
• Plug-and-play installation
• Voice enabled (Cisco 827-4V)
  - VoIP on four FXS interfaces
  - VoATM ready (AAL2)
  - G.711, G.729, G.723.1 voice codecs on all four FXS ports
  - Voice signaling: H.323 at FCS; VoATM/AAL2, SGCP, MGCP and CLASS features in 2H/CY ’00
Cisco 827 Architecture

**Chassis**
- One ADSL DMT Issue 2 Port-Based on Alcatel DynaMiTe Chipset
- One Ethernet Port
- Console Port
- RISC Processor MPC855T @ 50 MHz
- Locking Connector on Power Socket
- Kensington Compatible Locking Slot

**Optional Voice Ports**
- 4 FXS Voice Ports
- VoIP Now, Software Upgrade Toot in 2H/CY ’00
- G.711, G.729, G.723.1 Voice Codecs
- H.323 Today, SGCP/MGCP and CLASS Features in 2H/CY ’00

**Memory**
- Runs from DRAM
- DRAM Onboard/default: 16 MB for 827, 24 MB for 827-4V
- DRAM Max: 32 MB
- Flash Onboard/Default: 12 MB
- Flash Max: 20 MB

**Interoperability**
- Cisco DSLAMs
- Lacteal and Lucent DSLAMs Based on Alcatel Chipsets

**Differentiated Classes of Service**

**Application-Aware Networking**

- **Benefit:**
  Differentiate how bandwidth is used based on application, department, or user

- **Key features:**
  - IP QoS
    Class-Based Weighted Fair Queuing (CBWFQ)
    Committed Access Rate (CAR)
  - ATM QoS
    CBR, VBR (real-time and non-real-time), UBR
Differentiated Classes of Service

**Traffic Management**

- **Benefit:**
  - Limit how much bandwidth is allocated to a specific application.
  - Allows service providers total backbone bandwidth for bandwidth-intensive applications, e.g., video and voice.

- **Key Features:**
  - Per VC queuing
  - Per VC traffic shaping
  - Weighted Random Early Detection (WRED)

Integrated Toll-Quality Voice/Data

**Award-Winning Toll-Quality Voice**

- Same technology used in the award-winning AS5300 VoIP gateway.

- Multilayer prioritization of traffic: ATM, PPP, and IP
  - Per VC queuing, VBR (real time and non-real time), PPP fragmentation and interleaving, CBWFQ, RSVP, WRED

- Optimized DSP-based voice compression
  - Codecs: G.711, G.729, G.723.1
Integrated Toll-Quality Voice/Data

- **Standards-based technology**
  Enables ecosystem of third parties to develop applications to a standard
  Ecosystem provides complete solution for rapid deployment of voice services

- **Key features**
  H.323 standards-based signaling with RAS
  SGCP/MGCP for signaling to centralized industry-standard call agents
  Channel Associated Signaling (CAS)

Small-Office Value-Added Internet Access

- High-Speed Internet Access
- Videoconferencing
- Prioritized Traffic for Mission-Critical Hosted Applications Such as Customer-Relations Management
- Business-Class Secure Access

Small Office Cisco 827

Service Provider Network

Application Service Provider

Hosted Applications

Internet

www.salesforce.com

Videoconferencing

User

User
Voice Application Scenarios
Small Offices and Telecommuters

Small Offices
Cisco 6400
POTS/PSTN
Cisco 6100/6200
ATM/Packet Core
ISPs
Corporate
PSTN

Telecommuter
Cisco 827-4V
POTS Splitter/Micro Filter
Key System
IP Phone
POTS Splitter/Micro Filter

Standards-Based Derived Voice for
Small Offices and Telecommuters

Small Office
Key System
Cisco 827-4V
Gatekeeper
DSLAM
H.323 RAS
IP/ATM Network
PBX
Corporate Gateway
Cisco 3600
Telecommuter
Cisco 827-4V

• Intranet toll-quality voice
• Connect analog phones directly or via key system
• PBX extension
Deploying Multiservice Networks, VPNs, and DSL in Small Enterprise Branch Offices and Small/Medium Businesses

Session 2308

Please Complete Your Evaluation Form

Session 2308