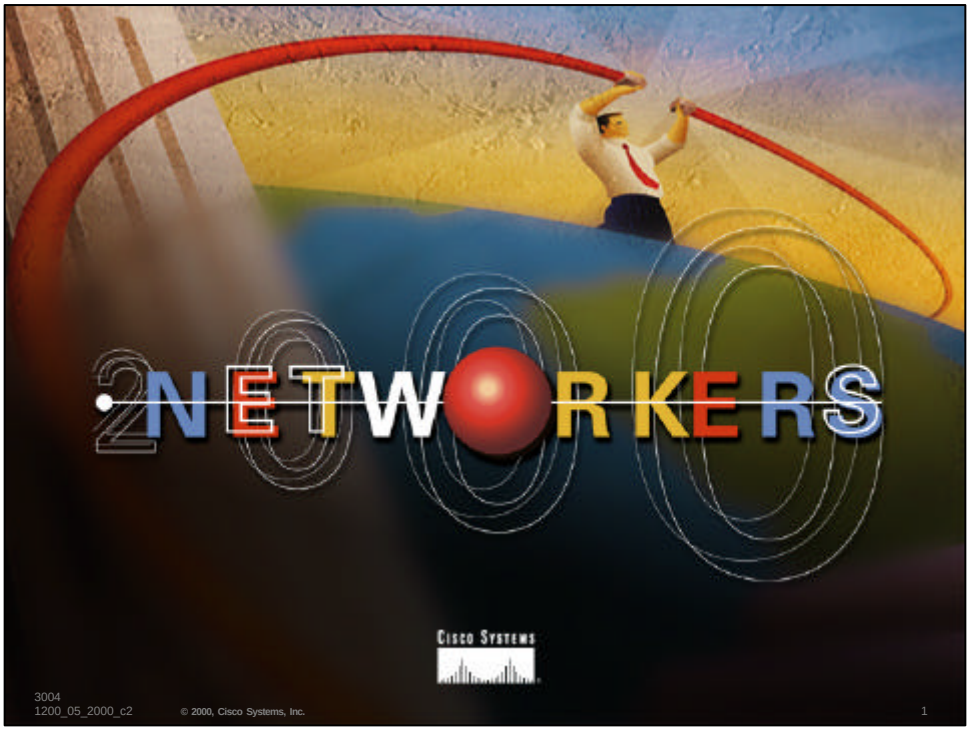


© 2000, Cisco Systems, Inc.

Design Principles for Very Large Wholesale Dial Services

Session 3004

Cisco Systems

© 2000, Cisco Systems, Inc.

Agenda

- Wholesale Dial Market
- Architecture Overview
- Design Issues
  - SS7 Integration
  - Port Policy Management
  - IP Addressing and Routing
  - Preventing Spam and DoS attacks
  - RADIUS Integration
- Summary

© 2000, Cisco Systems, Inc.

Market Trends

- "Free" Internet services changing business models for ISPs (especially in Europe)
- Evolution of service provider from transport supplier to enabling enterprise e-commerce through "virtual ISPs"
- Emergence of application service providers (ASPs) offering unified messaging, Find Me-Follow Me, and fax services
- Wholesale representing greatest market opportunity for service providers

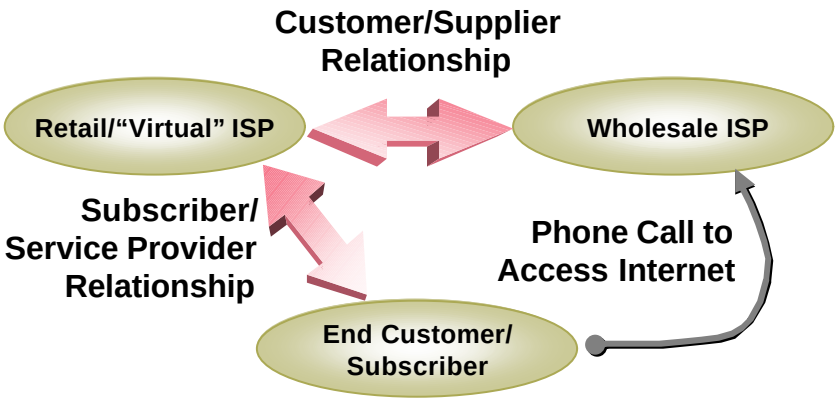
© 2000, Cisco Systems, Inc.

What Is Wholesale Dial?

- Wholesale ISP provides “virtual dial ports” to retail ISPs
- Subscribers get Internet access (i.e. not a VPN service)
- Retail ISP owns relationship with user base

© 2000, Cisco Systems, Inc.

The Wholesale Dial Relationship Triangle



© 2000, Cisco Systems, Inc.

Who Is Buying Wholesale Dial?

- **Enterprises**

  Dial access as channel to customers

- **Virtual ISPs/“dot coms”**

  Add dial access to service bundle

- **Other dial service providers**

  Extend range/reach

  Accelerate time to market

© 2000, Cisco Systems, Inc.

Buyer: Enterprise Private Label Internet

- **Example: Kmart (US), Dixons (UK), JB Oxford (US), Deutsche Bank (Germany)**
- **Free Internet as a channel for reaching customers**
- **NOT providing access for company employees to corporate network**
- **Control access = control customer**
- **Cost of providing access comparable to or less than cost of TV/news/radio advertising**

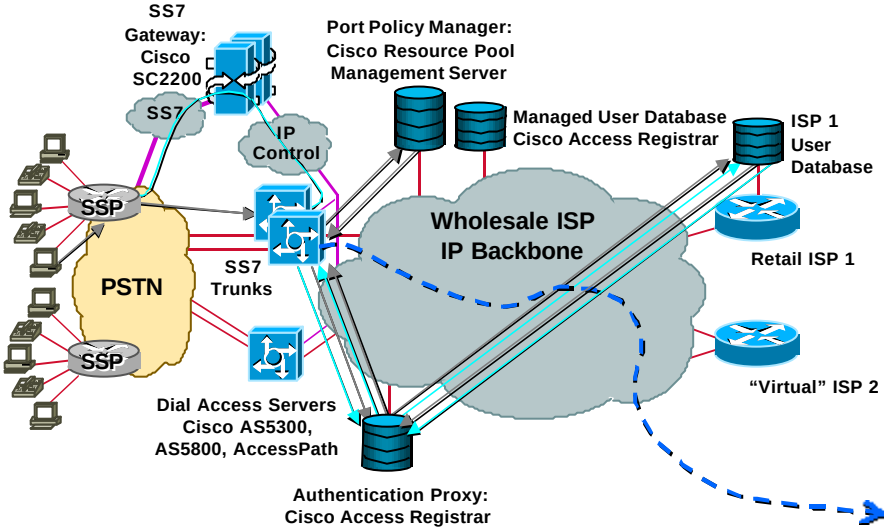
© 2000, Cisco Systems, Inc.

The Role of Intermediaries in Private Label Internet Access

	Advertiser Supported		Subsidized
	Consumer Free Internet Services	Enterprise Private Label Internet Services	Employee Internet Services
Brand	altavista, LYCOS, NETZERO	DELL net, E*TRADE, BLUE LIGHT, JBOxford & COMPANY	Ford Motor Company, intel, AmericanAirlines
Internet Service Enablers	1stUp.com free the web, spinway.com, freei		peoplepc
	Cisco Powered Network		

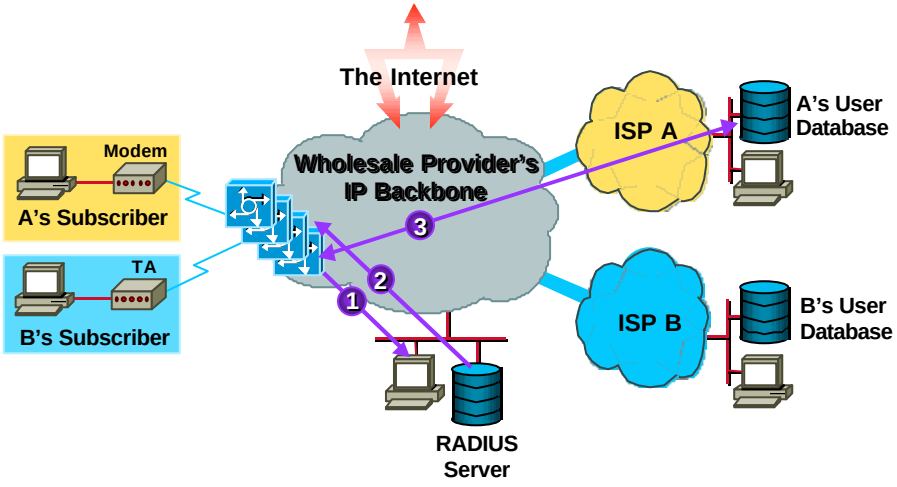
© 2000, Cisco Systems, Inc.

A Day in the Life of a Wholesale Dial Call



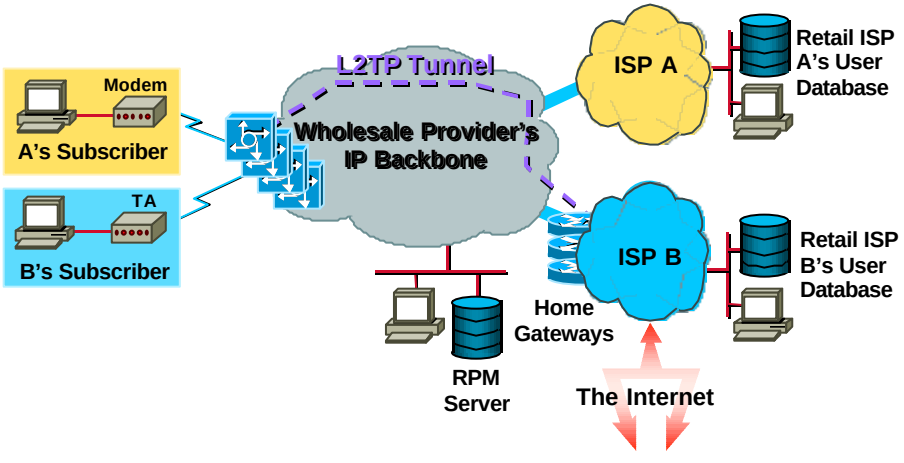
© 2000, Cisco Systems, Inc.

RADIUS-Only Wholesale Dial



© 2000, Cisco Systems, Inc.

Wholesale Dial with Tunnels



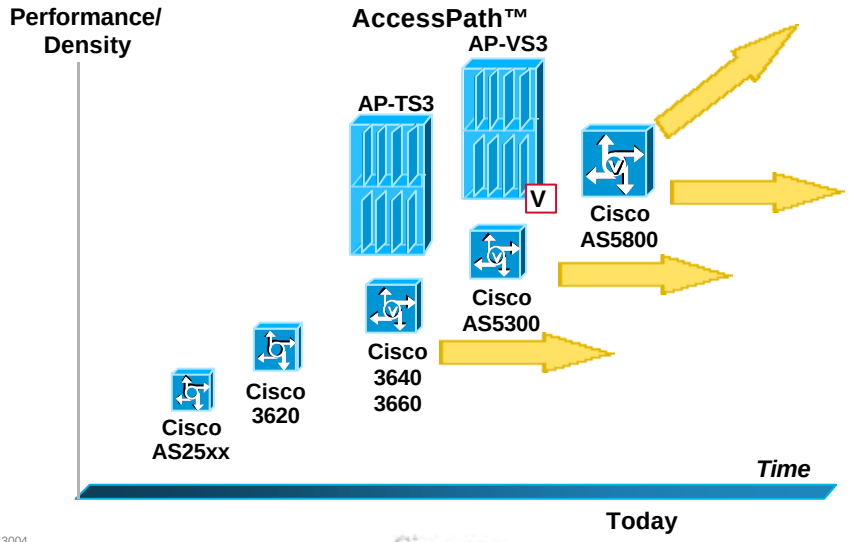
© 2000, Cisco Systems, Inc.

Design Considerations

- SS7 integration
- Port policy management
- IP addressing and routing
- RADIUS integration

© 2000, Cisco Systems, Inc.
Cisco.com

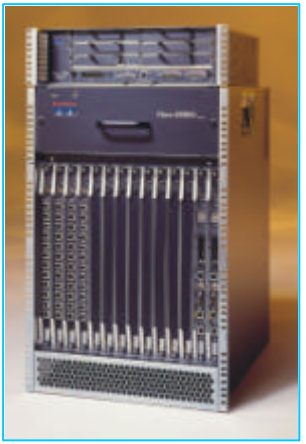
Dial Access Server Products



© 2000, Cisco Systems, Inc.
Cisco.com

AS5800 Platform Description

- Carrier-class remote access concentrator
  - Hot swap on all cards
  - Redundant power, modems, line cards, controllers
  - Up to 1440 calls (up to 48 T1/E1 ports or 2xCT3)
- Power and flexibility is key to services
  - High performance for multimedia/voice applications
  - QoS features: NetFlow, RSVP, IP precedence, WFQ
  - Dial VPN features: L2F, L2TP, IPSec, GRE, tag
  - Universal backhaul: FE, Serial, HSSI, ATM
  - SS7 integration for large scale
- Integrates with existing access servers
  - Cisco IOS stacking software enables true scalability and investment protection
  - Cisco stacking technology: MMP, SGBP, L2F
  - Same user interface and management as AS5200/AS5300



© 2000, Cisco Systems, Inc.

Dial Shelf

- 14 slots with hot-swap on all cards
- Front-to-back airflow
- Redundant fan modules
- Load balancing, redundant DC or AC power supplies

© 2000, Cisco Systems, Inc.

Router Shelf

- Router shelf is a Cisco 7206 (VXR)
- Performs packet forwarding and routing functions
- Houses backhaul port adapters
- Houses service adapters
- Hot swap on all PAs and SAs

© 2000, Cisco Systems, Inc.

AccessPath-VS3 and -TS3 System Overview

- **Completely integrated solution**
  - Dial, switching, backhaul routing, system controller
  - Configurator—quick deployment, user-friendly configuration
- **Scalability**
  - CT1/PRI data port capacity: 192 to 4032 (6*T3)
  - CE1/PRI data port capacity: 240 to 5040
  - CT1/PRI VoIP port capacity: 96 to 1008
  - CE1/PRI VoIP port capacity: 120 to 1260
  - Integrated gatekeeper (optional)
- **High availability**
  - Feature shelves: hot swap and RPS
  - Gatekeepers: HSRP
  - DASA: no single point of failure
- **NEBS compliant**

© 2000, Cisco Systems, Inc.

Cisco AS5300

- Dial/voice access server
- Data 196/240 ports (T1/E1)
- Voice 48/60 ports (T1/E1)
- Cisco IOS software
- Two RU height
- Redundant power
- NEBS/ETSI compliant

© 2000, Cisco Systems, Inc.

Cisco 3600 Series

- RISC-based architecture
- 50–70-kpps fast switching
- 3–4-kpps process switching
- Four network module slots
- Up to 128-MB DRAM

Versatility
Integration
Performance

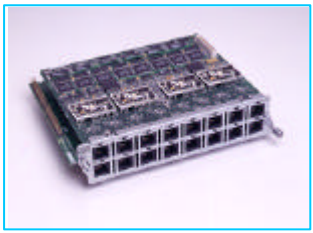
- RISC-based architecture
- 20–40-kpps fast switching
- 1.5–2.0-kpps process switching
- Two network module slots
- Up to 64-MB DRAM

© 2000, Cisco Systems, Inc.

Cisco 3600/2600 Analog Dial Interfaces

- 8 or 16 V.34 analog modems; up to 48 modems in a Cisco 3640
- Up to 16 modems in a Cisco 2600
- Integrated dial-and-routing solution for small and medium businesses, workgroups, and small ISPs

Cisco 3600/2600 Series

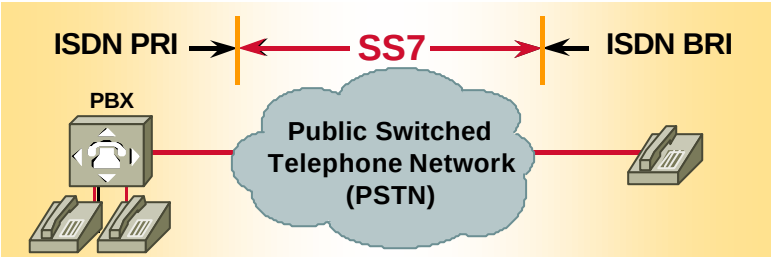


© 2000, Cisco Systems, Inc.

SS7/C7 for Dial Access

© 2000, Cisco Systems, Inc.

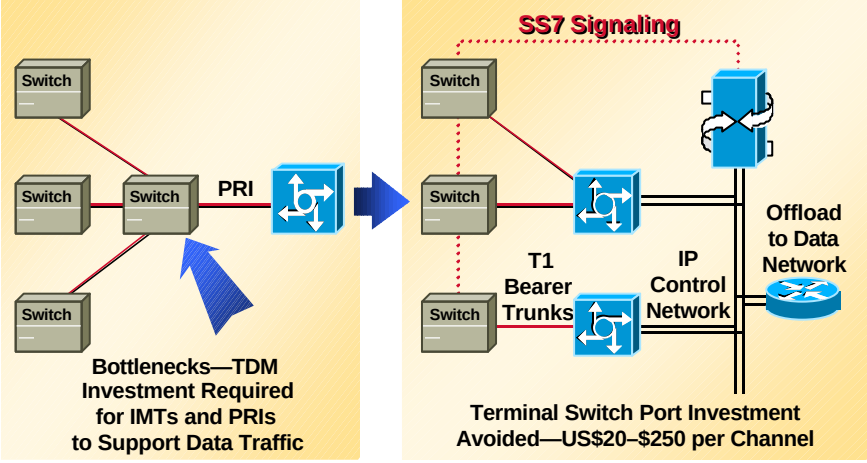
What Is SS7/C7?



- Chosen PSTN signaling protocol—used worldwide
- Provides look ahead and circuit reservation
- Sets up calls and tracks call status
- Accesses databases (800, local number portability) and intelligent network services (e.g. voice VPN)
- Highly scalable—designed for telephony scale

© 2000, Cisco Systems, Inc.
Cisco.com

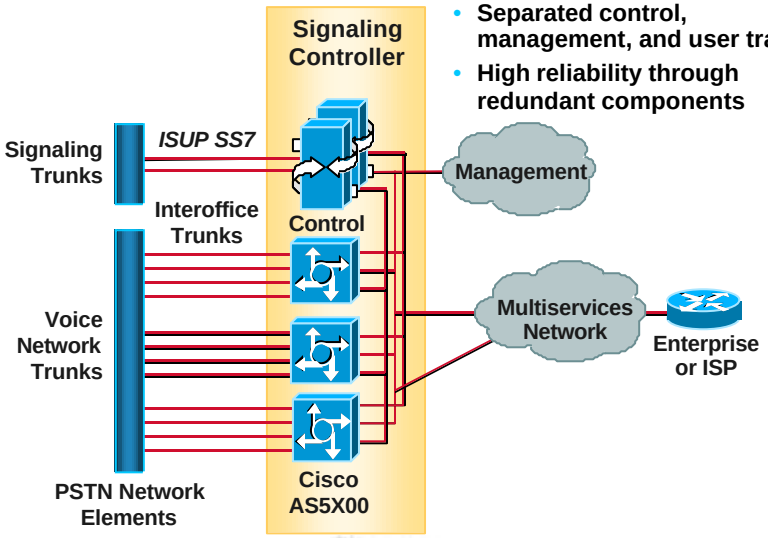
Cisco SC2200 Reduces Telco Switch Congestion



© 2000, Cisco Systems, Inc.
Cisco.com

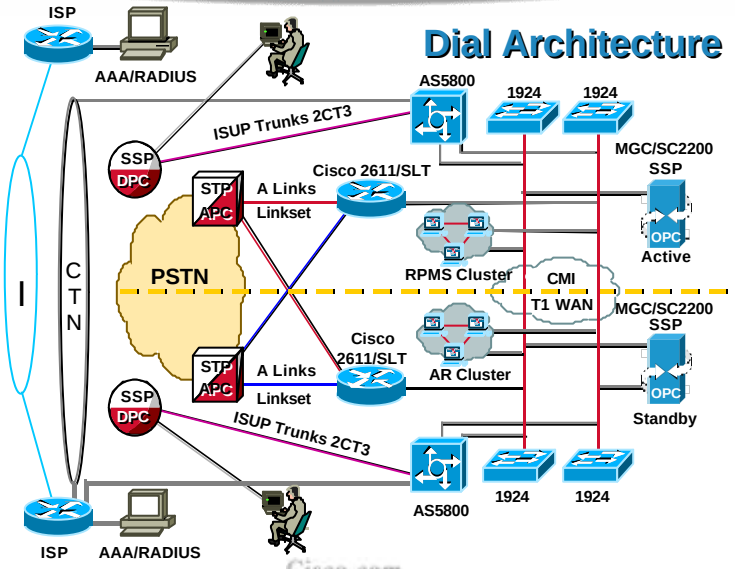
Cisco SC2200 Signaling Controller Architecture

- Separated control, management, and user traffic
- High reliability through redundant components



© 2000, Cisco Systems, Inc.

Detailed SS7 Architecture



© 2000, Cisco Systems, Inc.

SC2200 Benefits the ISP

- "Reciprocal compensation" available in some countries
- ISPs getting much better PSTN charges with SS7 (10–75% lower)
  - Carriers benefit because they relieve congestion and free up PRIs
  - Regulations may dictate lower SS7 interconnect rates
- Potential for fewer busy signals

© 2000, Cisco Systems, Inc.

© 2000, Cisco Systems, Inc.

Resource Pooling Capabilities

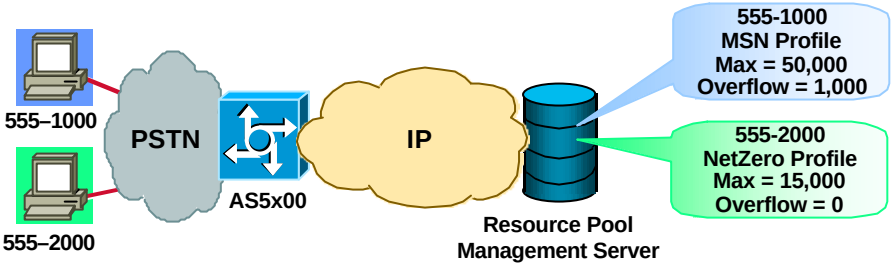
- Call filtering (before call is answered)

- Port availability guarantees

- Data over Speech Bearer Service (DOSBS)

© 2000, Cisco Systems, Inc.
Cisco.com

Cisco Resource Pool Management



- Port policy management for wholesale dial providers
- Enables service level agreements
  - Maximum number of active ports
  - Overflow capacity
  - Call detail records with overflow flagging
  - Flexible Web-based reporting for retail ISPs

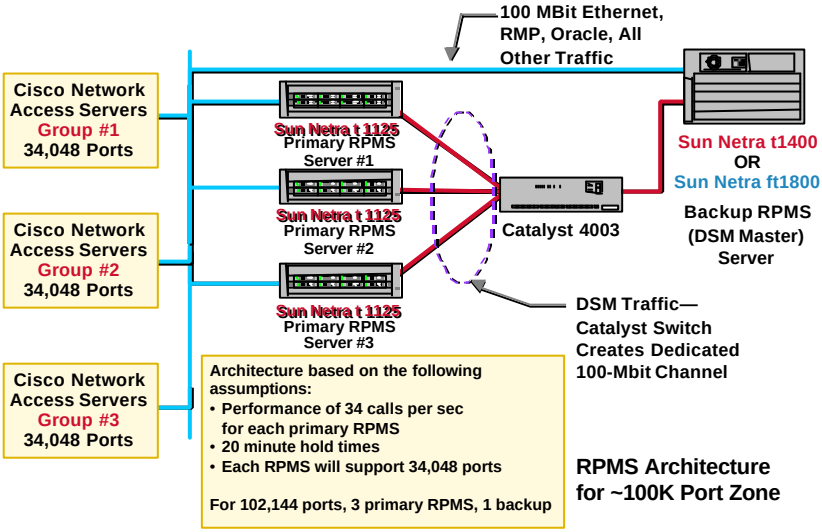
© 2000, Cisco Systems, Inc.
Cisco.com

Fault Tolerance and Resiliency

- No RPMS, no calls answered
- Database replication
  - Synchronizes back-end database records
- Multiple RPMS servers (primary/secondary)
  - Distributed Session Management Protocol
  - Synchronizes state of primary and secondary RPM servers
- Call context reconstruction
  - NAS retains enough information to reconstruct correct counters on secondary after failure

© 2000, Cisco Systems, Inc.
Cisco.com

Detailed RPMS Redundancy Architecture



RPMS Architecture for ~100K Port Zone

© 2000, Cisco Systems, Inc.
Cisco.com

© 2000, Cisco Systems, Inc.

How Dial IP Routing Works in Cisco IOS

- PPP assigns IP address to end user
  - Part of IPCP negotiation
- Host route on NAS for every dial user
  - Relatively large number of /32 routes
  - Frequent NAS route table changes
- IP addresses assignment alternatives:
  - Server-defined IP address pool
  - RADIUS-defined IP address pool
  - Per user according to AAA profile

© 2000, Cisco Systems, Inc.

Dial IP Routing Guidelines

- Summarize and advertise routing prefix to backbone
  - Minimize backbone route recalculations
- Use classless routing protocol
  - For example: OSPF, EIGRP, IS-IS
  - Minimizes advertised routing prefixes
- Don't propagate /32s to backbone unless *absolutely necessary*

© 2000, Cisco Systems, Inc.

Wholesale Dial IP Addressing and Routing

- Wholesale dial provider owns address space
  - Follow dial IP routing guidelines
- Retail ISPs provide address space
  - Use L2TP tunneling
- Mostly own, some retail ISP-provided
  - Address pools (with care), L2TP

© 2000, Cisco Systems, Inc.

Retailer-Provided IP Address Space

- Must aggregate addresses into larger blocks for routing sanity
- Don't know where users are going to "land" on the network
- Can't aggregate with per-user IP addressing
- Use L2TP to tunnel users to retailers network

© 2000, Cisco Systems, Inc.

© 2000, Cisco Systems, Inc.

Stopping E-Mail Spammers

- ACL configured on the access server blocks non-local SMTP

```
ip access-list extended NoSPAM
   permit tcp any 192.168.55.0 0.0.0.255 eq smtp
   deny   tcp any any eq smtp log
   permit ip any any
```

- Enabled in the RADIUS "user" file

```
spamford Password = ”wallace"
        Service-Type = Framed,
        Filter-Id = "NoSPAM.in",
        Framed-Protocol = PPP,
        Framed-MTU = 1500
```


© 2000, Cisco Systems, Inc.
Cisco.com

Disconnect Problem Users with "Packet of Death"

- Enables remote disconnect of problem users
- Send NAS a RADIUS packet on port 1700
- Uses IDs from RADIUS accounting file

```
Sun Apr 11 11:53:39 1999
        NAS-IP-Address = 10.65.106.167
        NAS-Port = 49
        ...
        Acct-Session-Id = "1010013BE"
        Framed-Protocol = PPP
        POD-Session-Key = "DD62C63D"
        Acct-Delay-Time = 0
```

Accounting session ID

Packet Of Death key ID

© 2000, Cisco Systems, Inc.
Cisco.com

"Packet of Death" (Cont.)

- Enable on NAS with command

  aaa pod server key *<key>*

- RADIUS packet must contain:

  User ID

  POD key

  MD5 hash (computed using RADIUS shared secret key)

- Optionally contains

  Accounting session ID

  IP address

© 2000, Cisco Systems, Inc.
Cisco.com

Denial of Service Prevention: Stopping IP Address Spoofing

- Problem:

  Hackers launching attacks forge source IP

  Smurf attack can use low bandwidth link

- Solution:

  Reverse path filtering (part of CEF)

  Drops packets with forged IP source addresses

  CEF on AS5800/5300 in IOS 12.0T

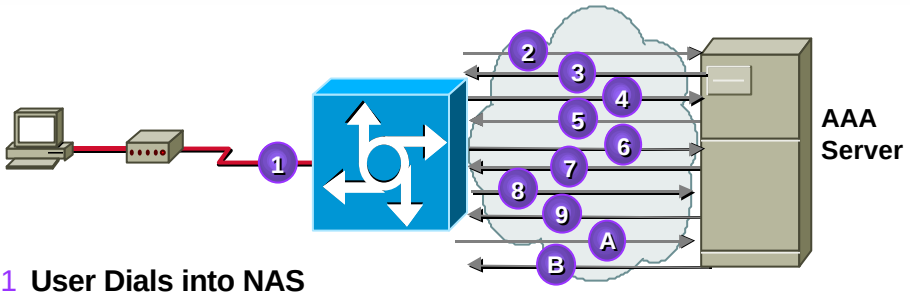
```
*Nov  4 111043.439 CEF-Receive Packet for
172.21.13.110 -- receive
*Nov  4 111043.439 CEF-Drop Packet from 10.1.1.10 via
Serial1/1/023 -- unicast rpf check
*Nov  4 111045.423 CEF-Receive Packet for
172.21.13.110 -- receive
*Nov  4 111045.423 CEF-Drop Packet from 10.1.1.10 via
Serial1/1/023 -- unicast rpf check
```


© 2000, Cisco Systems, Inc.
Cisco.com

RADIUS Authentication and Accounting

© 2000, Cisco Systems, Inc.

NAS and RADIUS Interaction



1 User Dials into NAS
2 Pre-Authentication Request
3 Pre-Authentication Accept
4 Authentication Request
5 Authentication Accept
6 Accounting Request (START)
7 Accounting Request Accept
8 Accounting Request (INTERMEDIATE)
9 Accounting Request Accept
A Accounting Request (STOP)
B Accounting Request Accept

© 2000, Cisco Systems, Inc.

RADIUS Requests in Wholesale Dial

- **Pre-authentication**

  Wholesaler decides whether to take call

- **Authentication**

  Retailer decides whether to accept user

- **Accounting**

  Start, intermediate, stop accounting

  For both retailer and wholesaler

© 2000, Cisco Systems, Inc.

Preauthentication

- **Introduced in Cisco IOS 11.3(10)AA, finalized in Cisco IOS 12.0(7)T**
- **Authenticates calls using DNIS**

```
aaa preauth
   dnis password Cisco-DNIS
```

```
1015551234 Password = "Cisco-DNIS", Service-Type = Outbound
        Service-Type = Outbound, Class = "ISP01",
        Cisco:Ascend-Require-Auth=Require-Auth
```


© 2000, Cisco Systems, Inc.

Preauthentication RADIUS Packet Trace

```
15:32:05.644549 nas07.radius > tusk.radius: Access-Request ID: 102 PLen: 117
    NAS-IP-Address [4]              Len:6     10.65.106.167
    NAS-Port [5]                    Len:6     54
    VSA:Cisco:Cisco-NAS-Port [26,9,2]         Len:19/13 "Serial1:22*"
    NAS-Port-Type [61]              Len:6     ISDN-Sync [2]
    User-Name [1]                   Len:12    "1016719406"
    Called-Station-Id [30]          Len:12    "1016719406"
    Calling-Station-Id [31]         Len:12    "1017770875"
    User-Password [2]               Len:18    73 34 c0 ec 57 62 0a 70 96 2f 21 c4 64 c5 f8 45
    Service-Type [6]                Len:6     Outbound [5]
    Acct-Session-Id[44]             Len:10    "0A001782"

  15:32:05.690623 tusk.radius > nas07.radius:  Access-Accept  ID: 102 PLen: 33
    Class [25]                      Len:7     "ISP01"
    Service-Type [6]                Len:6     Outbound [5]
```


© 2000, Cisco Systems, Inc.

Multivendor RADIUS Support

- Critical to integrate with retailers with existing dial ports
- Configuration

  radius-server host non-standard

  radius-server vsa send

  radius-server attribute nas-port format c

© 2000, Cisco Systems, Inc.

Wholesale/Retail Correlated Accounting Records

- **Logging the IP address in the accounting START record**

  aaa accounting delay-start

- **Consistent port reporting across pre-authentication and accounting records**

  radius-server attribute nas-port format c

  radius-server attribute 44 on-for-access-req

```
 1             0
5 4 3 2 1 0 9 8 7 6 5 4 3 2 1 0
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
F F S S S S L L L L L C C C C C
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+

FF    = shelf (0-3)
SSSS  = slot (0-15)
LLLLL = line (0-31)   <-- the DS1#, even within a CT3
CCCCC = channel (0-31)
```


© 2000, Cisco Systems, Inc.

© 2000, Cisco Systems, Inc.

Troubleshooting Essentials

- Four commands to run on any dial access server:

```
no logging console
service timestamps debug datetime msec
service timestamps log datetime msec
modem call-record terse
```

- Ensures debugging is nonservice affecting
- Enhances value of debug information
- Allows establishment of call failure patterns (Cisco IOS 11.3AA and 12.0T only)

© 2000, Cisco Systems, Inc.

Conditional Debug

- *Essential* for larger access servers
- Allows debug to be turned on and off based upon:
  - Username
  - Calling number/called number
  - Interface

```
debug condition {username username | called
                                  dial-string | caller dial-string}
debug condition interface "interface"
```


© 2000, Cisco Systems, Inc.

Debugs Affected by Conditions

debug aaa {accounting | authorization | authentication}

debug dialer {events | packets}

debug isdn {q921 | q931}

debug modem {oob | trace}

debug ppp {all | authentication | chap | error | negotiation | multilink events | packet}

© 2000, Cisco Systems, Inc.
Cisco.com

Active User Information

Show caller ({ interface *name* [full] | username *name* [detailed] | line *range* [full] | ip })

```
5300# show caller username mary
User: mary, line Vi1, service PPP Bundle, active 00:00:18
  PPP: LCP Open, multilink Open, IPCP
  Dialer: Connected 00:00:25 to 60222, inbound
        Idle timer 120 secs, idle 19 secs
        Type is IN-BAND SYNC, group Dialer0
  IP: Local 1.0.0.3/8, remote 10.1.1.1
  Bundle: First link of mary, 1 link, last input 00:00:19
  Counts: 3 packets input, 36 bytes, 0 no buffer
        0 input errors, 0 CRC, 0 frame, 0 overrun
        3 packets output, 36 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
```


© 2000, Cisco Systems, Inc.
Cisco.com

Modem Troubleshooting

- Factor out Layer 3/PPP issues
- Verify connectivity from Layer 1 upwards

  Check the T1/E1 before assuming modem problems
- Fix individual client modem problems through upgrades

  http://www.56k.com/

© 2000, Cisco Systems, Inc.

SS7 SLT Troubleshooting

debug ip udp	Verify connectivity with SC2200
debug ss7 mtp2 backhaul 0	Verify interactions between SLT and SC2200
debug ss7 mtp2 iac 0	Verify alignment *during SS7 link bringup*

© 2000, Cisco Systems, Inc.

SS7 SLT Point-Code Debugging

```
slt-pop1# debug ss7 mtp2 pac 0
    *Mar 6 18:37:50.650: ---- Incoming Rudp msg (35 bytes) ----
    SM_msg_type 0x00008000
    protocol_type 0x0001
    msg_ID 0x0000
    msg_type 0x0010
    channel_ID 0x0000
    bearer_ID 0x0000
    length 0x0013
    data 0xB2020202 0x01010100 0x11905472 0x616E7350
    0x61746800
```

Originating Point Code 2.2.2

Destination Point Code 1.1.1

© 2000, Cisco Systems, Inc.
Cisco.com

Verifying NAS↔SC2200 Connectivity

```
nas1-5300# deb rlm group 0

RLM Group debugging is on

nas1-5300 #
Feb 17 15:11:51.093: rlm 0: [State_Down, rx OPEN_WAIT_TIMEOUT
Feb 17 15:11:51.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] tx
ECHO_REQ(tid=6254)
Feb 17 15:12:06.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] tx
ECHO_REQ(tid=6259)
Feb 17 15:12:06.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] rx
ECHO_ACK(tid=6259)
Feb 17 15:12:06.093: rlm 0: [State_Down, rx LINK_OPENED] over link
[16.1.1.1(Ethernet0),16.1.1.20]
Feb 17 15:12:07.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] tx
ECHO_REQ(tid=6260)
Feb 17 15:12:07.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] rx
ECHO_ACK(tid=6260)
```


© 2000, Cisco Systems, Inc.
Cisco.com

Verifying SS7 Connectivity (Cont.)

```
Feb 17 15:12:09.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] tx
START_REQ(tid=0)
Feb 17 15:12:09.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20]
requests activation
Feb 17 15:12:09.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] tx
ECHO_REQ(tid=6262)
Feb 17 15:12:09.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] rx
START_ACK(tid=0)
Feb 17 15:12:09.093: rlm 0: [State_Down, rx START_ACK] over link
[16.1.1.1(Ethernet0),16.1.1.20]
Feb 17 15:12:09.093: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] is
activated
Feb 17 15:12:09.097: rlm 0: link [16.1.1.1(Ethernet0), 16.1.1.20] rx
ECHO_ACK(tid=6262)
Feb 17 15:12:09.097: %ISDN-6-LAYER2UP: Layer 2 for Interface
Se0:23 SC, TEI 0 changed to up
```

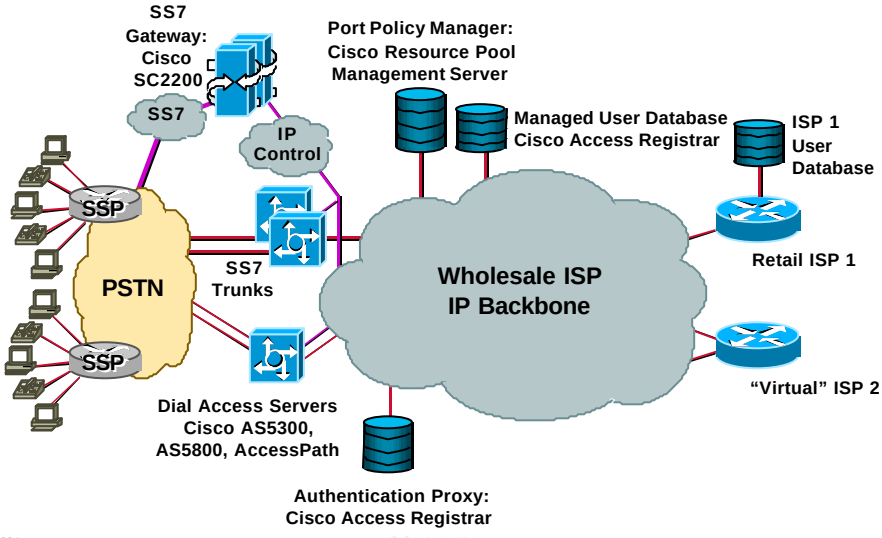

© 2000, Cisco Systems, Inc.

Performance Optimization for Dial Access Servers

- For best performance
  - Don't log to console
  - At least 10 AAA processes on AS5800
  - Enable CEF (FIB) switching
  - Use virtual profile precloning
  - Switch off VJ header compression
  - Always use conditional debug
  - Minimize dynamic routing
  - Minimize use of ACLs

© 2000, Cisco Systems, Inc.

Summary



© 2000, Cisco Systems, Inc.
Cisco.com

Summary

- **SS7 integration**
  - Reduce costs, improve scale
- **Port policy management**
  - Guarantee port availability
- **IP addressing and routing**
  - Minimize operational complexity
- **Prevent denial of service and spam**
  - Maximize service availability
- **RADIUS integration**
  - Key for network extension

© 2000, Cisco Systems, Inc.
Cisco.com

Contacts

- **http://www.cisco.com/**

  Everything that's official

- **Cisco-NAS@datasys.net**

  Not an official Cisco mailing list, but many technical Cisco staff read and respond daily

- **comp.dcom.sys.cisco**

  The oldest and still the most active list

© 2000, Cisco Systems, Inc.

Design Principles for Very Large Wholesale Dial Services

Session 3004

© 2000, Cisco Systems, Inc.

Please Complete Your Evaluation Form

Session 3004

© 2000, Cisco Systems, Inc.

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠

© 2000, Cisco Systems, Inc.