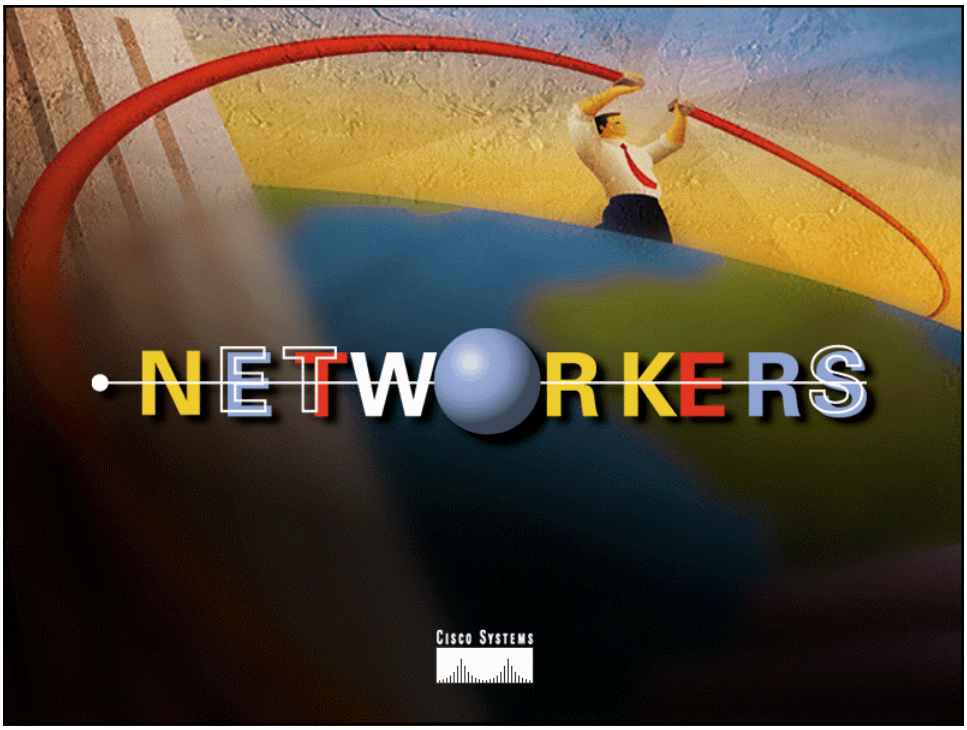


Agenda

- Dial Design Principles and Product Base
- Core Dial Technology
  - AAA, IP Routing, Virtual Private Networking, Service Level Agreements
- Putting It All Together
  - Wholesale Dial and Corporate Dial Outsource
- Miscellaneous Tips and Tricks
- SS7/C7 for Dial Access
- Summary

www.cisco.com

Core Dial Design Principles

- Centralize administration
- Distribute implementation
- Minimize IP routing complexity
- Maximize dial server performance
- Design for resiliency

www.cisco.com

At-a-Glance Dial Product Selector

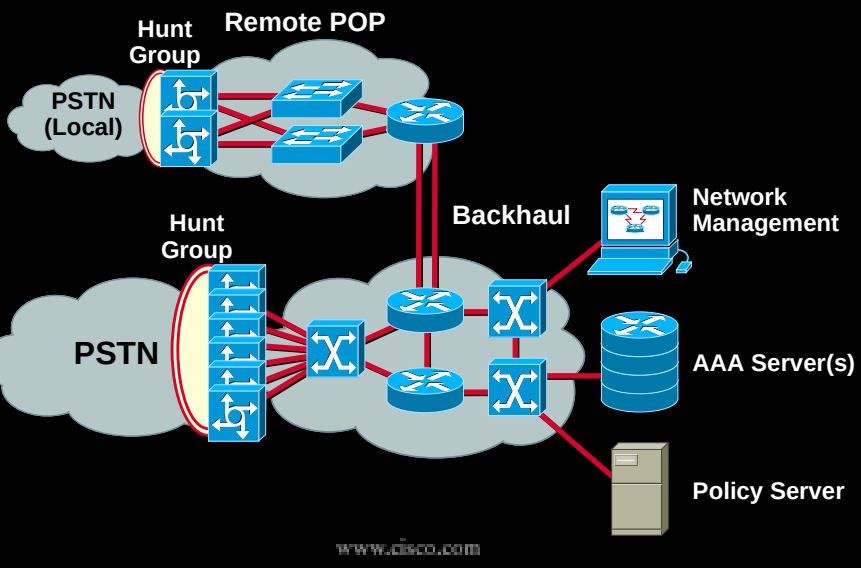
	Capacity (T1/E1)	2xBellcore Reliability	Redundancy Features	Main Processor	Interface Options	List Price per Port
AS5200	48/60	98.5%	None	20Mhz MC68030	T1/E1, 10BaseT, T1/E1 Serial	US$360
3640	48/60	99.83%	Redundant DC/AC Power	100Mhz R4700	T1/E1, 7000 Combinations	US$500
AS5300	192/240	99.98%	Redundant DC/AC Power	150Mhz R4700	T1/E1, 10/100BaseT, T1/E1 Serial	US$418
AS5800	1344/1440	99.999%	Redundant Modems, Controllers, Power	266Mhz R7000	T1/E1/CT3, Any 7200/7500 PA	US$437
AP-TS3	2496/3120	99.9999%	Redundant Shelves, Switch, Power	150Mhz R4700	T1/E1, Any 7200/7500 PA	US$457

www.cisco.com

Authentication, Authorization and Accounting (AAA)

www.cisco.com

Dial POP Reference Model



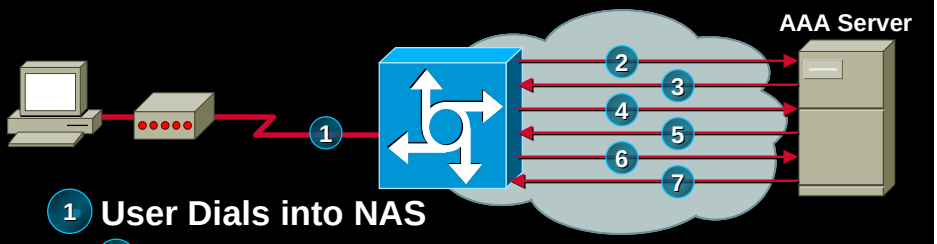
www.cisco.com

Centralize Administration: AAA Servers

- Provide centralized authentication, authorization, accounting
- AAA protocol choices
  - RADIUS
  - TACACS+
- AAA redundancy is critical
  - No AAA, no dial-in…no job!

www.cisco.com

NAS and AAA Interaction



1. User Dials into NAS
2. Access Request Message
3. Access Accept/Reject Response
4. Accounting Request (START)
5. Accounting Request Accept
6. Accounting Request (STOP)
7. Accounting Request Accept

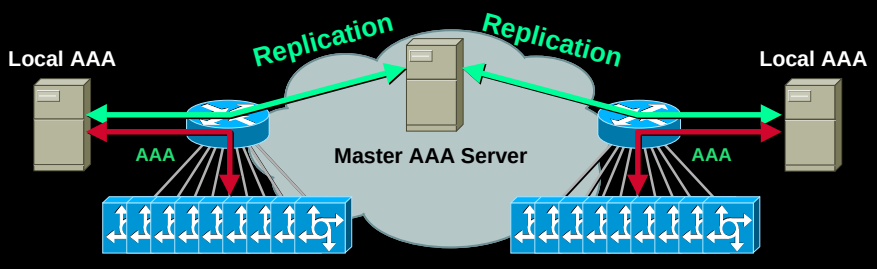
www.cisco.com

AAA Server Benefits

- Configure dial port on per-user basis
  - Applied when user connected
  - Discarded when user disconnects
- Centralized IP address admin
  - Configure address pools for NAS's
- Centralized accounting data
  - Feed into rating/billing application

www.cisco.com

Local AAA Servers



- Reduces delay, improves resiliency
- Balances load
- Failover to multiple AAA servers
- Requires server synchronization

www.cisco.com

Access Server AAA Scalability

- Increases number of AAA processes on access server
- Improves AAA throughput

```
aaa new-model
 radius-server host alcatraz
 radius-server key myRaDiUSpassWoRd
 radius-server configure-nas
 aaa authentication ppp dialins radius local
 aaa authentication login admins local
 aaa authorization network radius local
 aaa accounting network start-stop radius
 aaa processes 10
```

www.cisco.com

How Dial IP Routing Works in Cisco IOS®

- PPP assigns IP address to end user
  - Part of IPCP negotiation
- Host route installed 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

www.cisco.com

Dial IP Routing Guidelines

- Summarize and advertise routing prefix to backbone
  - Minimize backbone route recalculations
- Use classless routing protocol
  - E.g., OSPF, EIGRP, IS-IS
  - Minimizes advertised routing prefixes
- Don’t propagate /32s to backbone unless absolutely necessary

www.cisco.com

OSPF Summarization Example

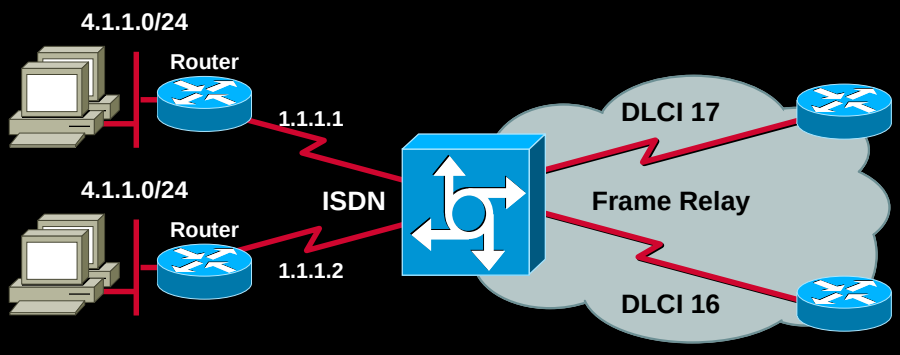
```
router ospf 1
 redistribute static metric 100 subnets
 network 10.21.102.0 0.0.0.255 area 0
!
ip local pool default 10.21.231.33 10.21.231.254
!
ip route 10.21.231.0 255.255.255.0 Null0
```

"Dust Magnet" Route

- Summarize host routes
- Drop rogue packets with "dust magnet"

www.cisco.com

Special Case: Remote LAN with Static Route



www.cisco.com

Static Remote LAN Routing via RADIUS

- Use Framed-IP-Address to set calling router IP address
- Use Framed-Route to install route for duration of call
- Classless routing protocol will advertise route to backbone

```
Framed-IP-Address = 1.1.1.1
Framed-Route = "4.1.1.0 255.255.255.0"
```


Dynamic Routing Updates from Remote Clients?

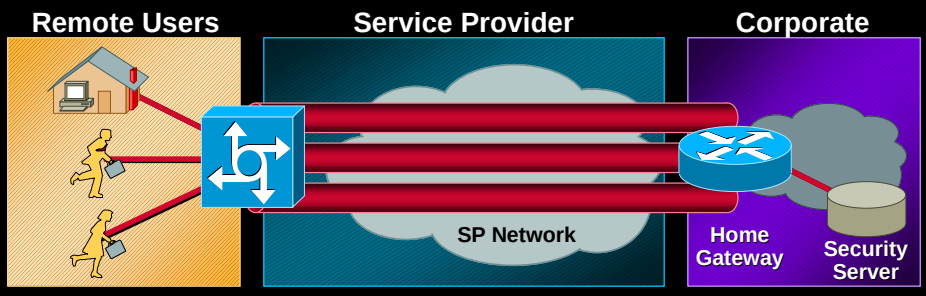
- **Don't do it!...**but if you really must
  - Set per-client flag in AAA profile to permit routing
  - Use route filtering—permit only default route
  - Consider passive-interface for asymmetric routing
  - Consider snapshot routing (RIP or IGRP) or on-demand OSPF
  - Consider route update authentication (MD5 hash)
  - NB: AS5800 only supports dynamic routing on 10% of interfaces at any one time

VPDN Protocol History

- **PPTP** (Point-to-Point Tunneling protocol) Microsoft/Ascend/3COM **Proprietary**
- **L2F** (Layer 2 Forwarding) Cisco **Proprietary (in Cisco IOS 11.2+)**
- **L2TP** (Layer 2 Tunneling Protocol)
  - IETF draft combining the best of PPTP
  - L2F industry standard track
- **IPSec** (IP Security)
  - AH mode (payload encryption)
  - Tunnel mode (entire packet encryption)

www.cisco.com

Point-to-Point Tunneling Protocol (PPTP)



Pros

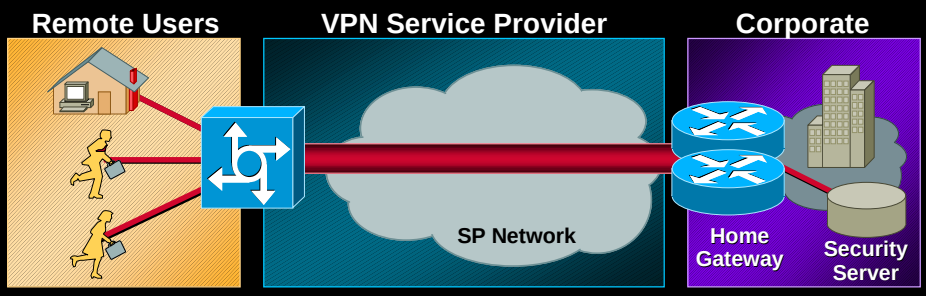
- No agreement with SP required
- Software included with Windows 98
- Completely under corporate control

Cons

- Software and config on remote PCs
- No QoS possible without SP
- Doesn't scale (one tunnel per user)

www.cisco.com

Layer 2 Tunneling Protocol (L2TP)



Pros

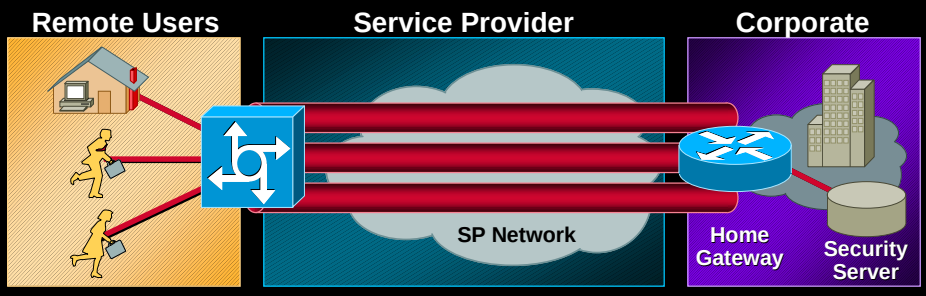
- No software changes on remote PCs
- Scales well, tunnel per NAS
- QoS techniques available
- Multiple home gateways for load balancing and redundancy

Cons

- Requires SP participation

www.cisco.com

Encryption (IPSec)



Pros

- No agreement with SP required
- Encryption for extra security
- Completely under corporate control

Cons

- Software and config on remote PCs
- No QoS possible without SP
- Export restrictions

www.cisco.com

VPN Technology Support in Cisco Dial Products

- **L2F**
  Release 11.2F onwards
- **L2TP**
  Release 11.3AA and 12.0, 12.0T
- **IPSec**
  Release 11.3T, 11.3AA, 12.0, 12.0T
- **PPTP**
  Not applicable—client initiated

www.cisco.com

Cisco Resource Pooling

- Enables dial service level agreements
  - Guaranteed port availability
  - Restricted/unrestricted overflow
  - Data-over-speech-bearer capability
- Flagging of overflow CDRs for billing and sales purposes
- Full HTML reporting capabilities

www.cisco.com

What Is a Resource?

- Anything in an access server that can terminate or originate a call
- Resource groups today:

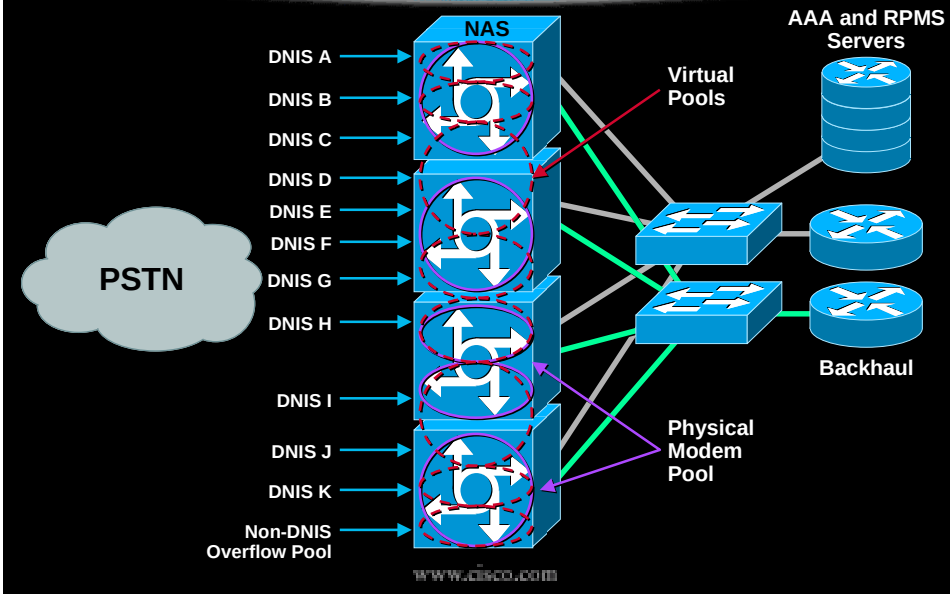
Modems	ISDN (HDLC) Controllers	V.110	V.120

- Future resource groups:

VoIP	Dial Out

www.cisco.com

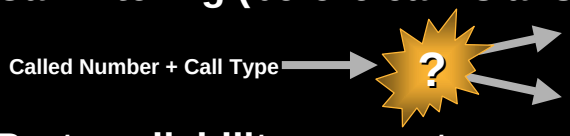
Resource Pooling Example



www.cisco.com

Resource Pooling Capabilities

- Call filtering (before call is answered)

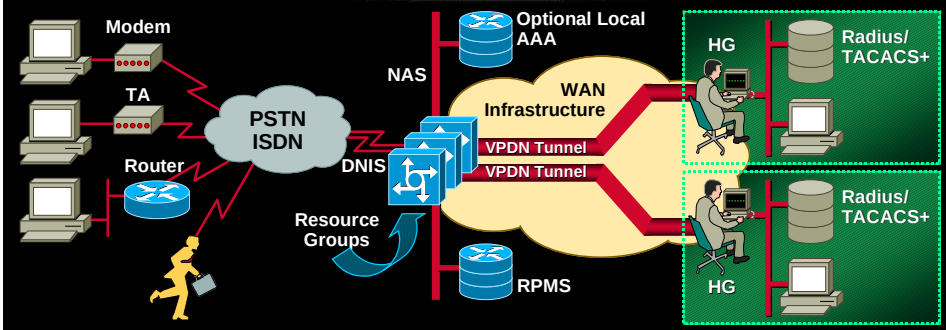


- Port availability guarantees

- Data-over-Speech-Bearer Service (DOSBS)

www.cisco.com

Example Resource Pooling Network



- Information captured at call setup
  - Called number (DNIS), call type, caller's number (ANI)
- All public network interfaces supported
  - PRI, CT1, CE1, SS7
- Resource pool management may be located
  - In the NAS (trivial case) or in a Resource Pool Manager Server

www.cisco.com

Resource Pool Manager Server

The Resource Pool Manager Server (RPMS) is a sophisticated resource manager that applies wholesale policies on a per-call basis. RPMS works alongside existing RADIUS or TACACS+ servers to apply wholesale customer profiles (policies) with high scalability.

www.cisco.com

Customer Profile

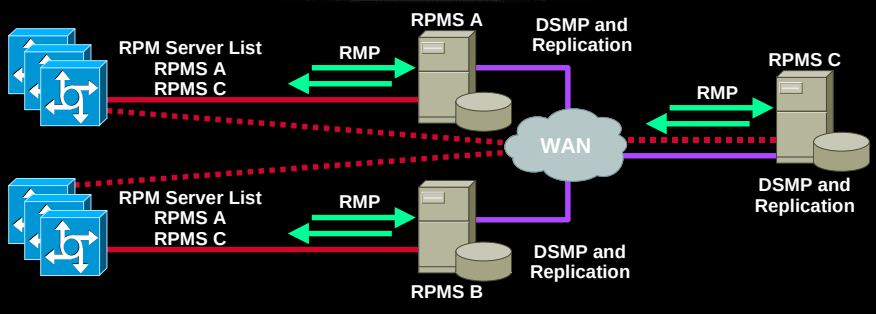
A customer profile is a record in the NAS or in the server that identifies a customer configuration. Fields in the record include the types of resources used by the customer's dial service plan and specify the maximum number of allowable sessions.

www.cisco.com

Fault Tolerance and Resiliency

- No RPMS, no calls answered…no job!
- 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

Fault Tolerance and Resiliency Example



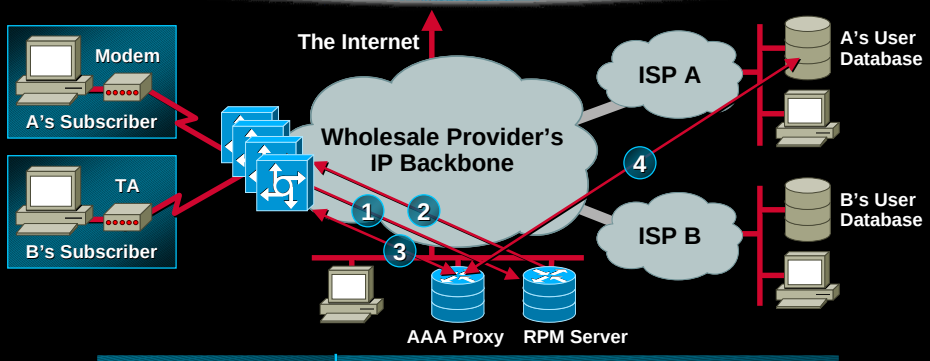
- Each NAS has a list of primary and backup RPMS IP addresses
- Resilient RMP is a peer-to-peer protocol between RPMS and NAS
- RPMS Distributed Session Management Protocol (DSMP) keeps synchronized resource pool data on primaries and the backup server
- Oracle database replication manager and RPMS cache update mechanism insures data is updated to all RPMSes
- Call context reconstruction between NAS and RPMS insures integrity of the call data between primary and backup RPMS

Putting It All Together
Service Examples

Wholesale Dial
Corporate Dial Outsource

www.cisco.com

Wholesale Dial



Service Attribute	Dial Technology
SLAs	Cisco Resource Pooling
Customer AAA Integration	GRS, Multivendor RADIUS Attributes
SS7 Connectivity	Signaling Controller 2200, COT Capability

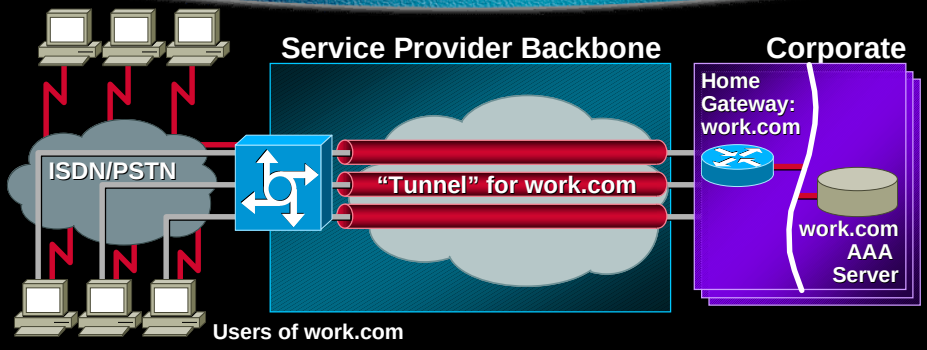
www.cisco.com

Wholesale Dial Benefits

- Customer (ISP) benefits
  - Outsource expensive activity
  - Reduce costs
  - Focus on differentiation
- Wholesaler benefits
  - Additional revenue opportunity
  - Leverage existing infrastructure
  - Reduce cost of sales per subscriber

www.cisco.com

Corporate Dial Outsourcing



Service Attribute	Dial Technology
Dial VPN	L2F, L2TP Tunneling
SLAs	Resource Pooling
Billing	RADIUS, TACACS+, RPMS

www.cisco.com

Corporate Dial Outsourcing

- Customer benefits
  - Outsource non-strategic activities
  - Maintain security and control
  - Reduce costs
- Service provider benefits
  - Additional revenue opportunity
  - Leverage existing infrastructure
  - Closer relationship with customers

www.cisco.com

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 non-service affecting
- Enhances value of debug information
- Allows establishment of call failure patterns (Cisco IOS 11.3AA and 12.0T only)

www.cisco.com

Conditional Debug
(Cisco IOS 11.3AA and 12.0T Only)

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

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

www.cisco.com

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}
```

www.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
```

www.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/

www.cisco.com

Performance Optimization for Dial Access Servers

- For best performance
  - Don’t log to console
  - At least 10 AAA processes on Cisco AS5800
  - Switch off virtual profiles
  - Switch off VJ header compression
  - Always use conditional debug
  - Minimize dynamic routing
  - Minimize use of ACLs

IP Address Pool Configuration Using RADIUS

- On the access server

```
aaa configuration config-username nas01
radius-server configure-nas
```

- In the RADIUS “user” file

```
pools-nas01     Password = "ascend"
        Service-Type = Outbound,
        Ascend:Ascend-IP-Pool-Definition = "1 192.168.0.32 8",
        Ascend:Ascend-IP-Pool-Definition = "2 10.12.0.32 8"
```

Assigning Users to IP Address Pools

- Select address pool within user's RADIUS profile
- Use for differentiated services

```
mary    Password = "contrary", NAS-Port-Type = Async
        Service-Type = Framed,
        Cisco:Ascend-Assign-IP-Pool = 2,
        Framed-Protocol = PPP,
        Framed-MTU = 1500
```

www.cisco.com

Controlling "Special" Users…

- ACL configured on the access server

```
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
```

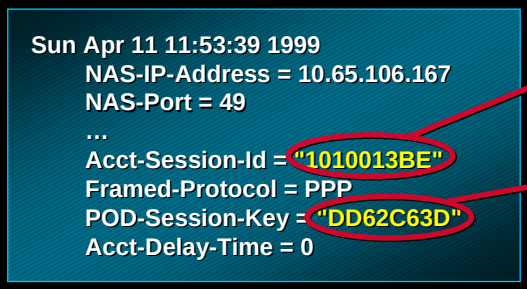
- In the RADIUS "user" file

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

www.cisco.com

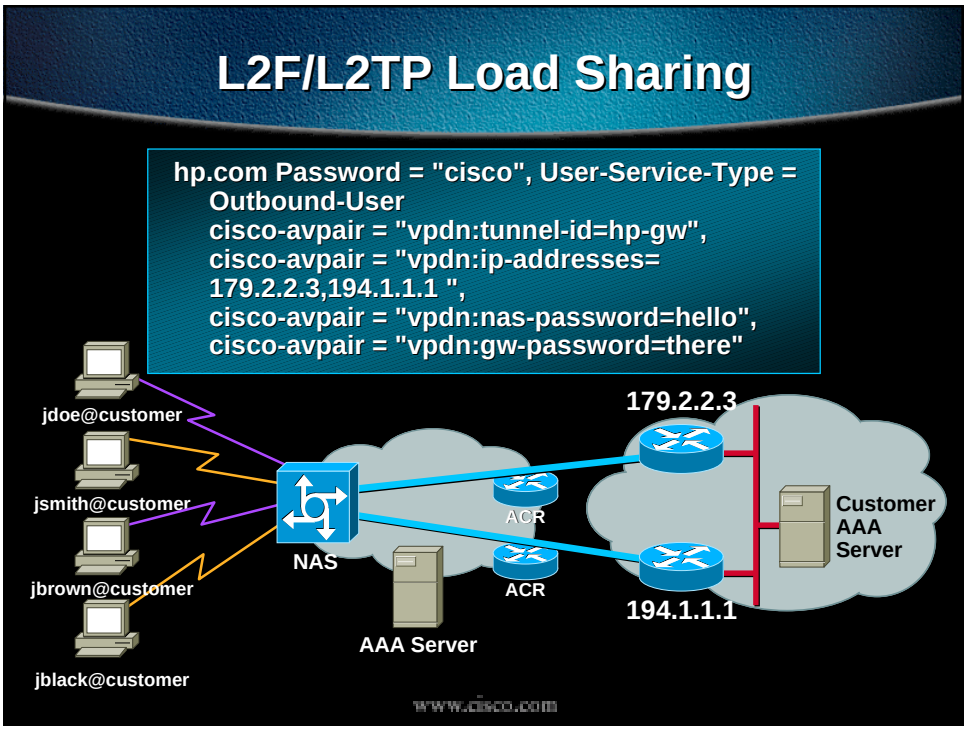
“Packet of Death” (POD)

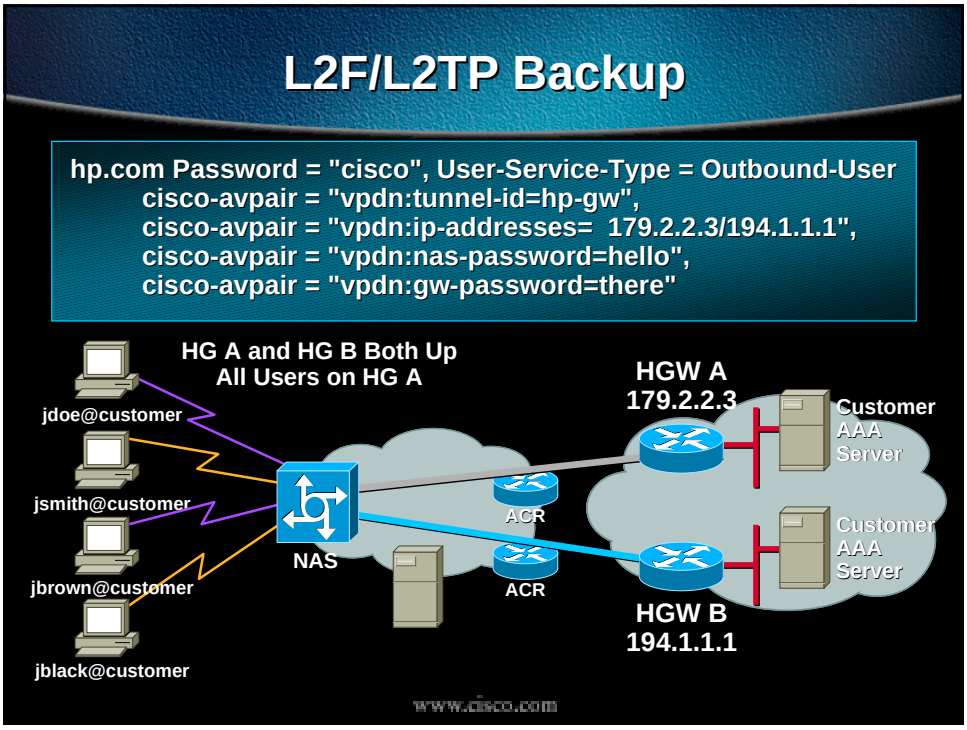
- Enables remote disconnect of problem users
- Send NAS a RADIUS packet on port 1700
- Uses IDs from RADIUS accounting file

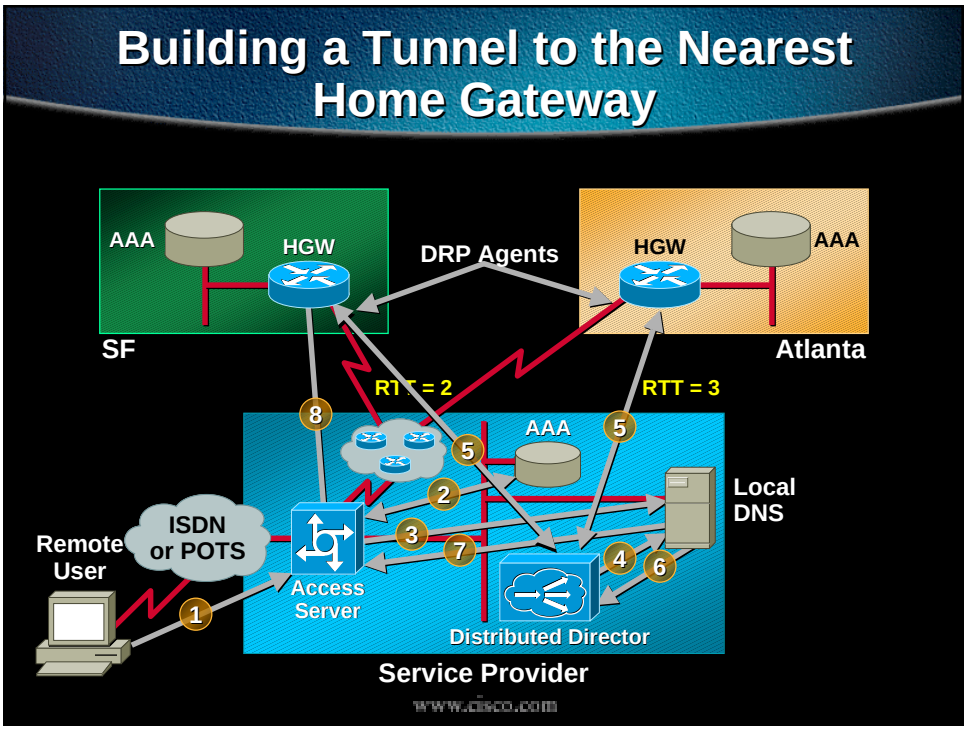


“Packet of Death” (Cont.)

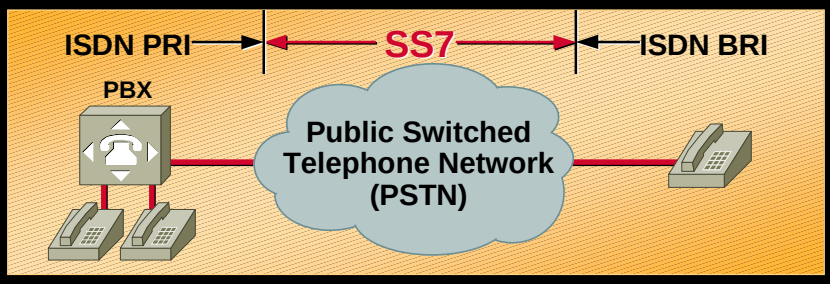
- Enable on NAS with command
  - aaa pod server key <*key*>
- RADIUS packet must contain
  - User ID
  - POD key
  - MD5 hash (computed using RADIUS shared secret key)
- Optionally contains
  - Accounting session ID
  - IP address







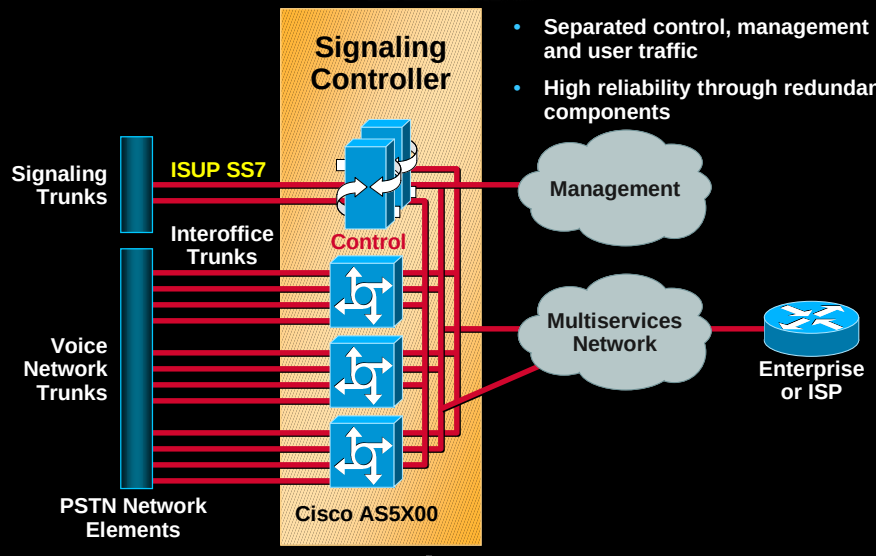
What Is SS7/C7?



- 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

www.cisco.com

Cisco SC2200 Signaling Controller Architecture



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

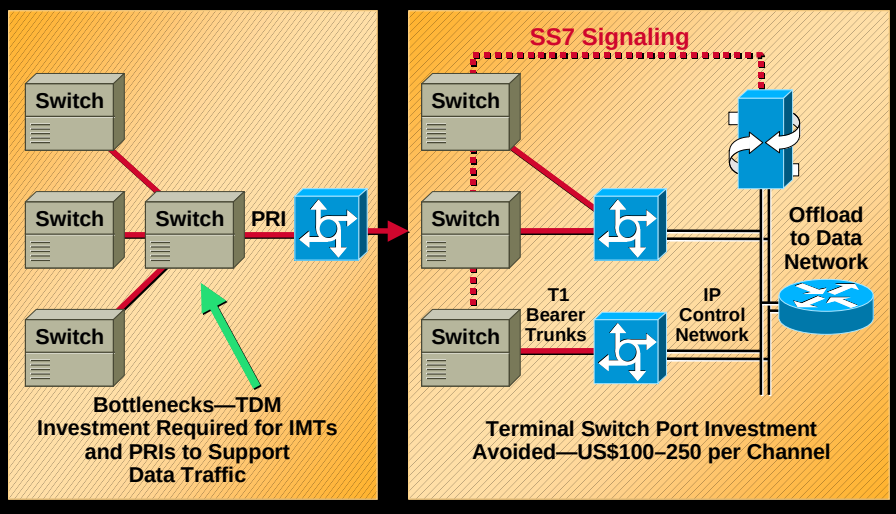
www.cisco.com

Service Provider Benefits of SS7/C7

- Lower network costs
- Improve network efficiency
- Implement the new dial access service model (wholesale dial)
- Lower carrier interconnect costs
- Improve the end user's experience

www.cisco.com

Cisco SC2200 Reduces Costs and Switch Congestion



www.cisco.com

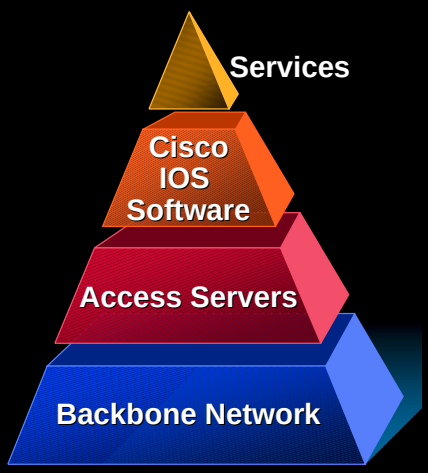
SC2200 Benefits the ISP

- Improved customer experience
- "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

www.cisco.com

Summary

- Centralize administration
- Distribute implementation
- Minimize IP routing complexity
- Maximize dial server performance
- Design for resiliency



www.cisco.com