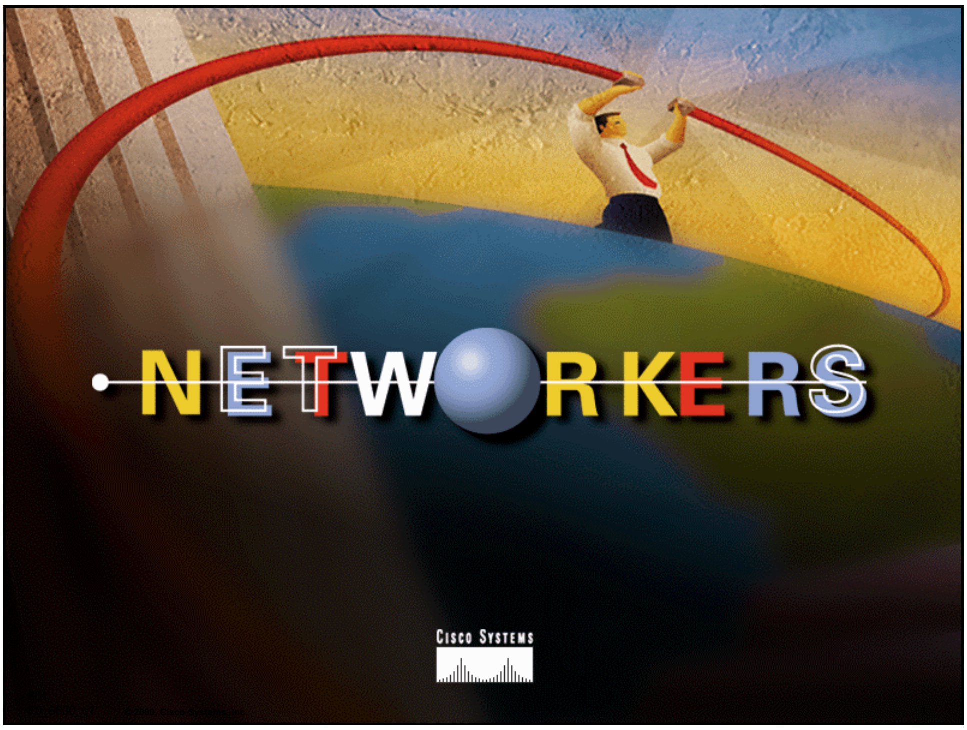


© 2000, Cisco Systems, Inc.

Evolution of Network Management Technologies

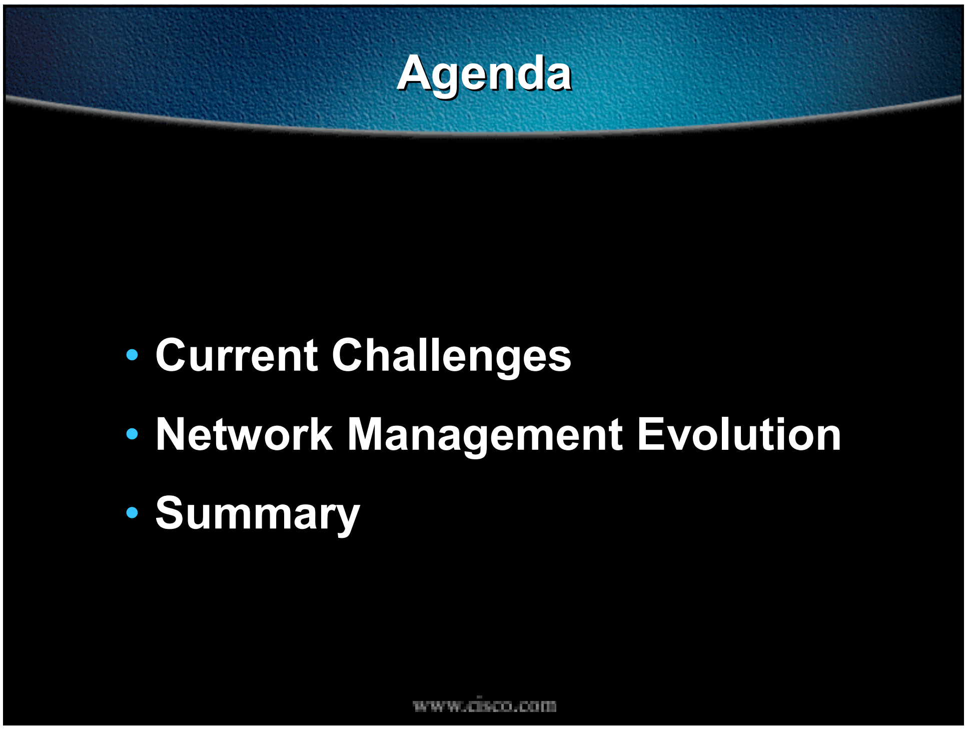
Session 801

801
F0_6630_c1 © 2000, Cisco Systems, Inc. 2

How Can We?

We can evolve the network management infrastructure to solve today's **scaling, security, interoperability,** and **service management** challenges.

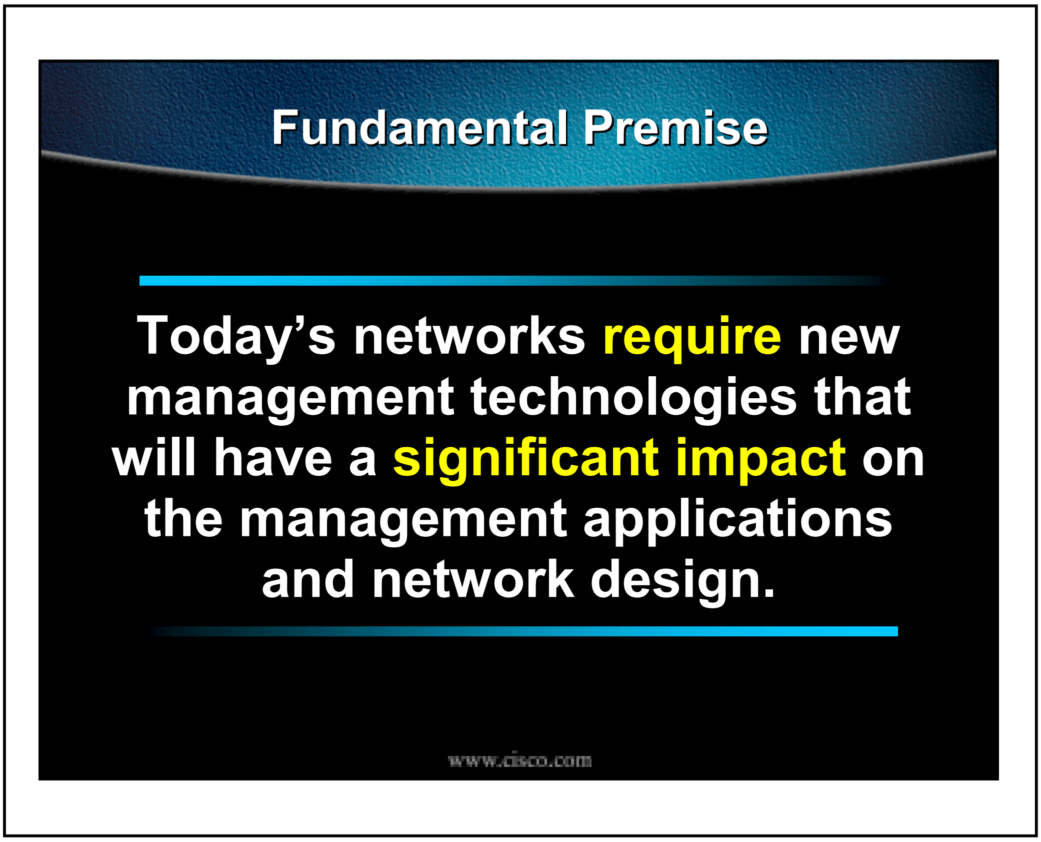
www.cisco.com



Agenda

- Current Challenges
- Network Management Evolution
- Summary

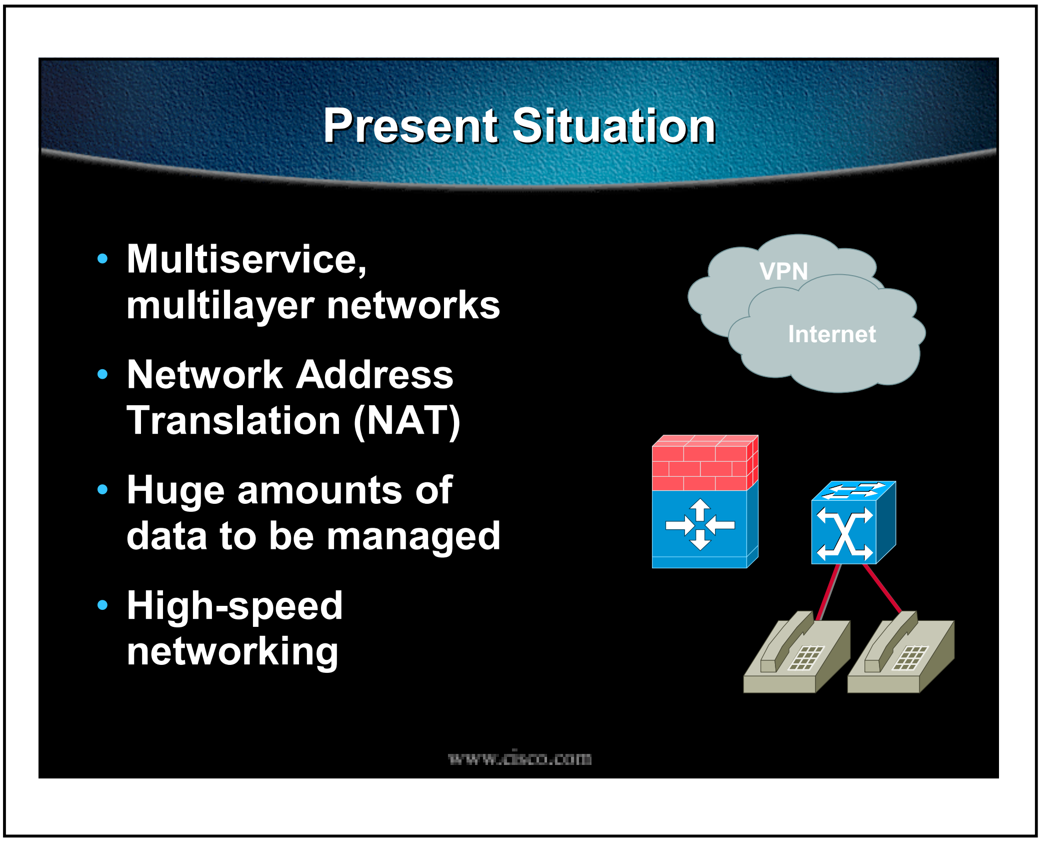
www.cisco.com



Fundamental Premise

Today’s networks **require** new management technologies that will have a **significant impact** on the management applications and network design.

www.cisco.com

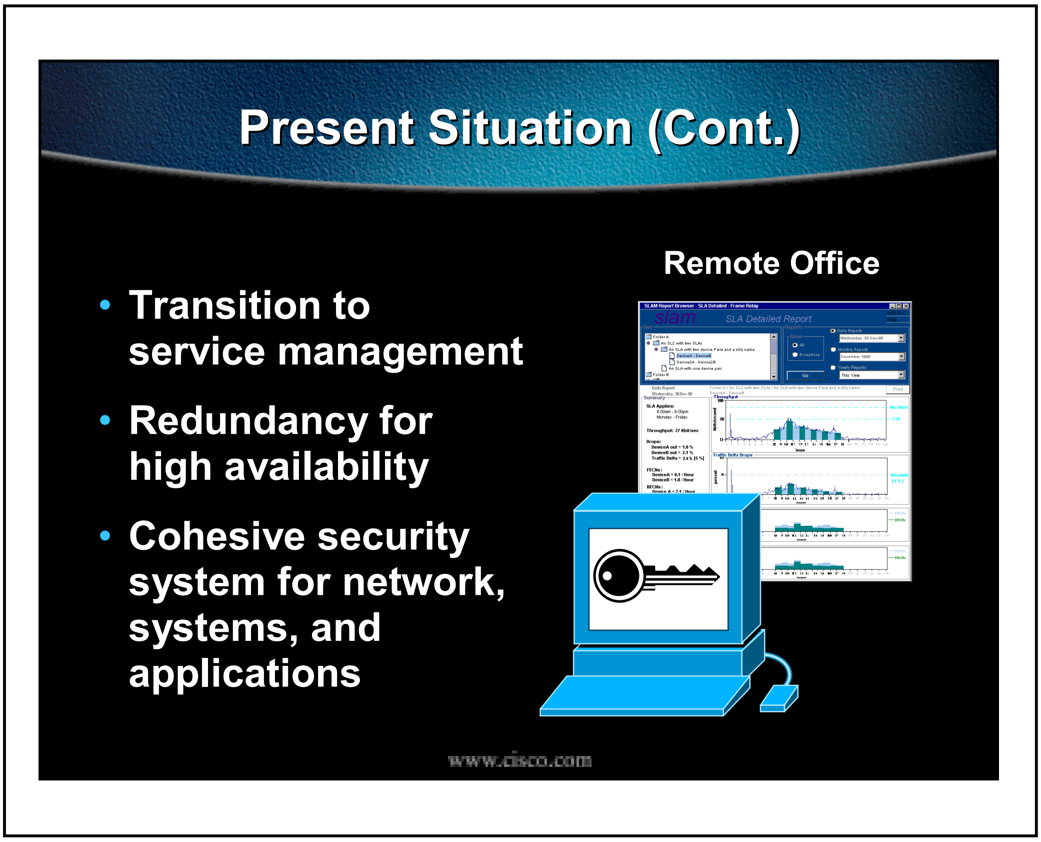


Present Situation

- Multiservice, multilayer networks
- Network Address Translation (NAT)
- Huge amounts of data to be managed
- High-speed networking

VPN
Internet

www.cisco.com

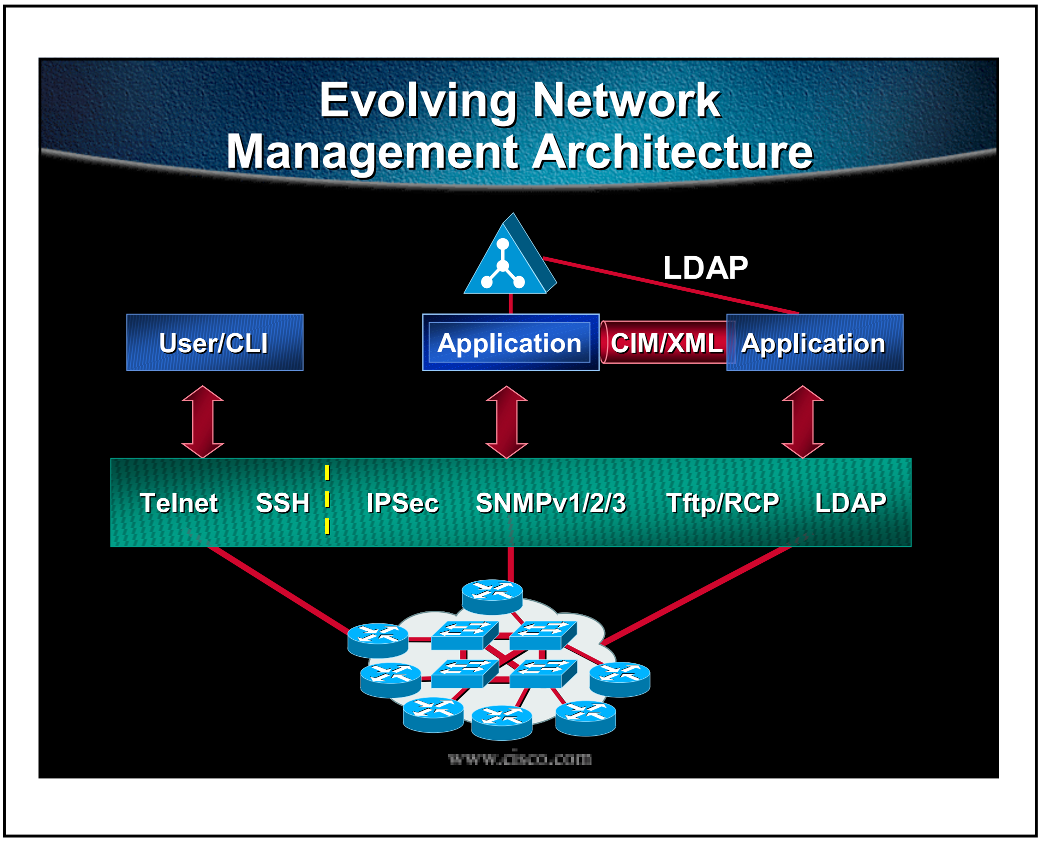


Present Situation (Cont.)

Remote Office

- Transition to service management
- Redundancy for high availability
- Cohesive security system for network, systems, and applications

www.cisco.com



Evolving Network Management Architecture

LDAP

User/CLI

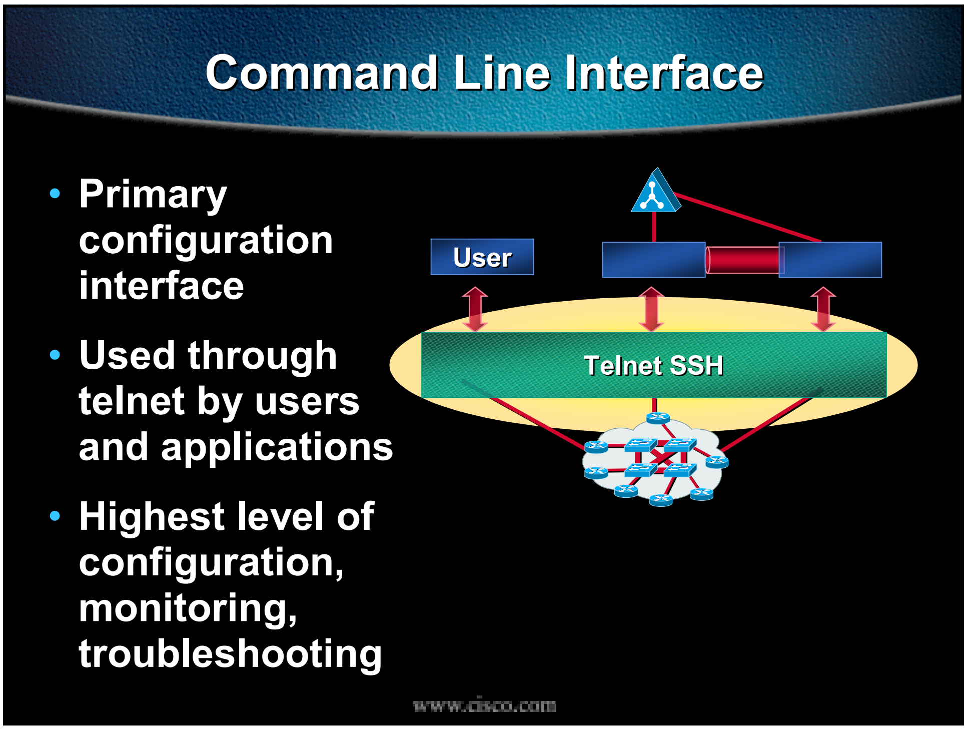
Application

CIM/XML

Application

Telnet SSH IPSec SNMPv1/2/3 Tftp/RCP LDAP

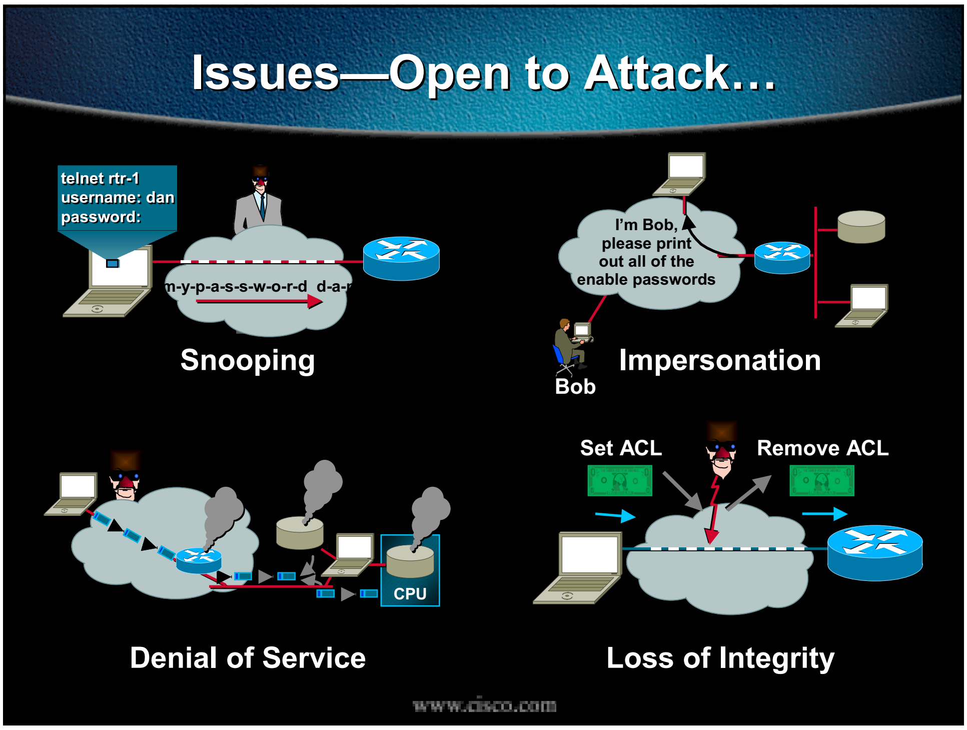
www.cisco.com



Command Line Interface

- Primary configuration interface
- Used through telnet by users and applications
- Highest level of configuration, monitoring, troubleshooting

www.cisco.com

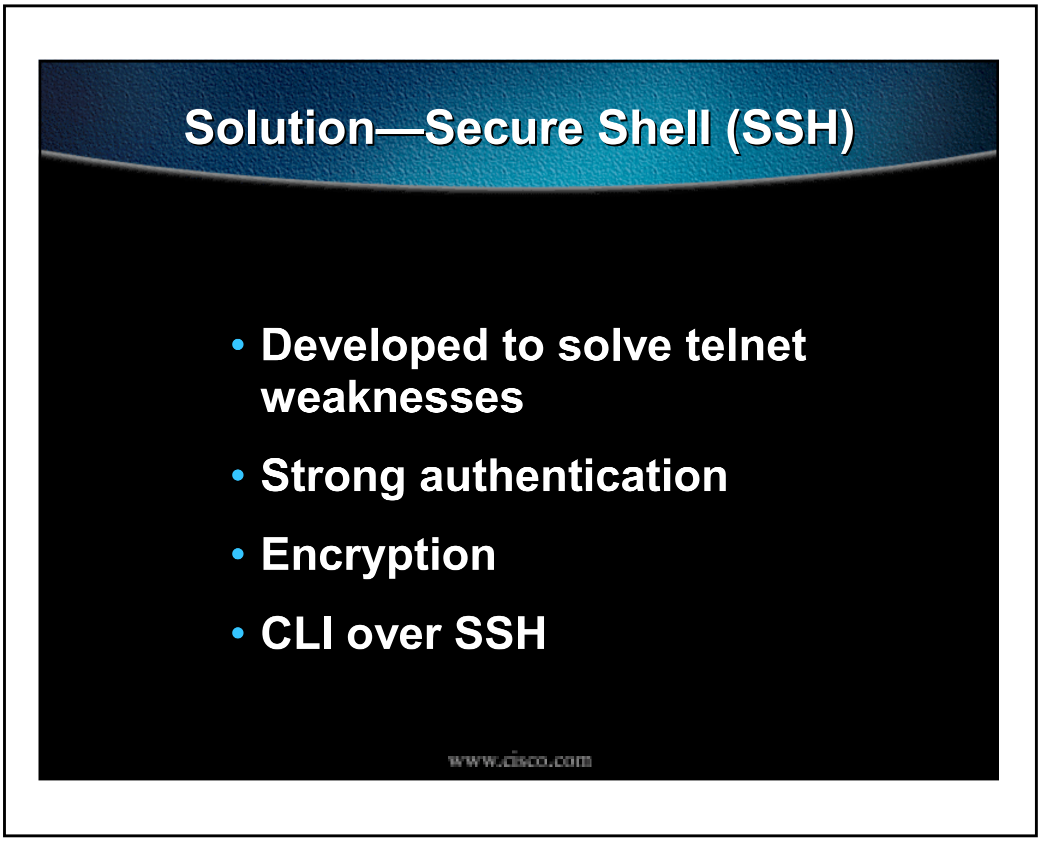


Issues—Open to Attack…

```
telnet rtr-1
username: dan
password:
```

m-y-p-a-s-s-w-o-r-d d-a-r
Snooping
I'm Bob, please print out all of the enable passwords
Bob
Impersonation
CPU
Denial of Service
Set ACL
Remove ACL
Loss of Integrity

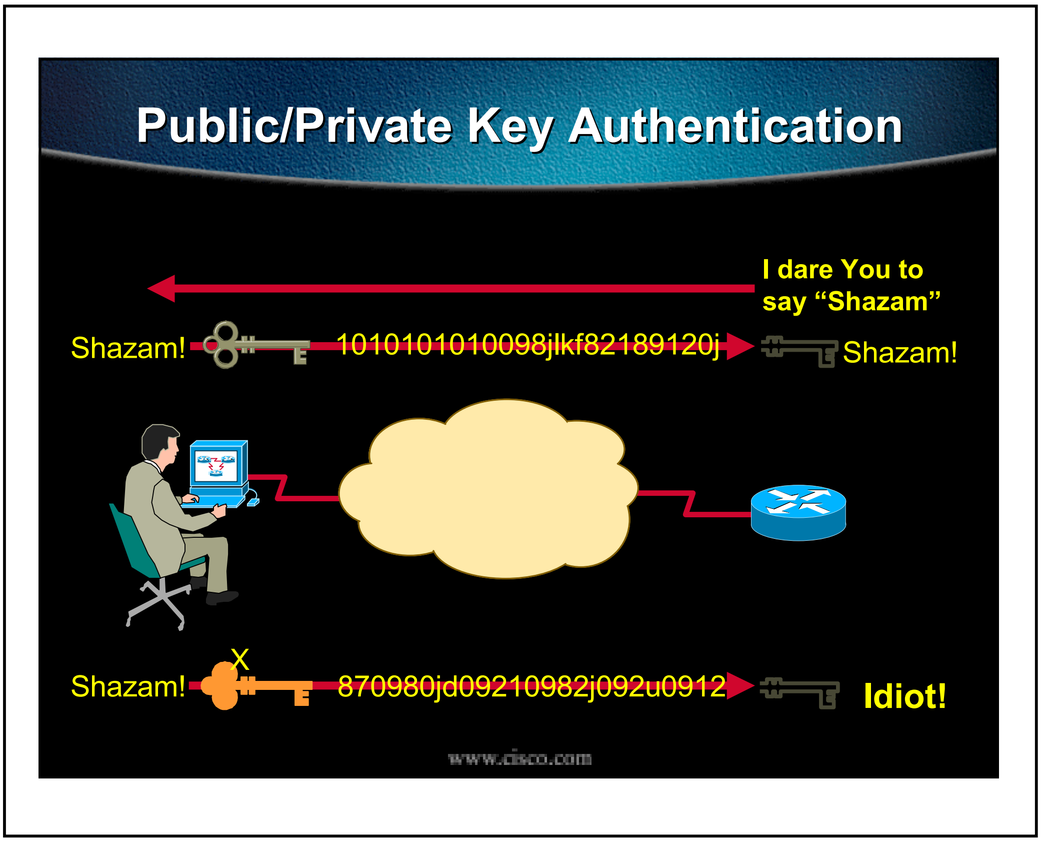
www.cisco.com



Solution—Secure Shell (SSH)

- Developed to solve telnet weaknesses
- Strong authentication
- Encryption
- CLI over SSH

www.cisco.com



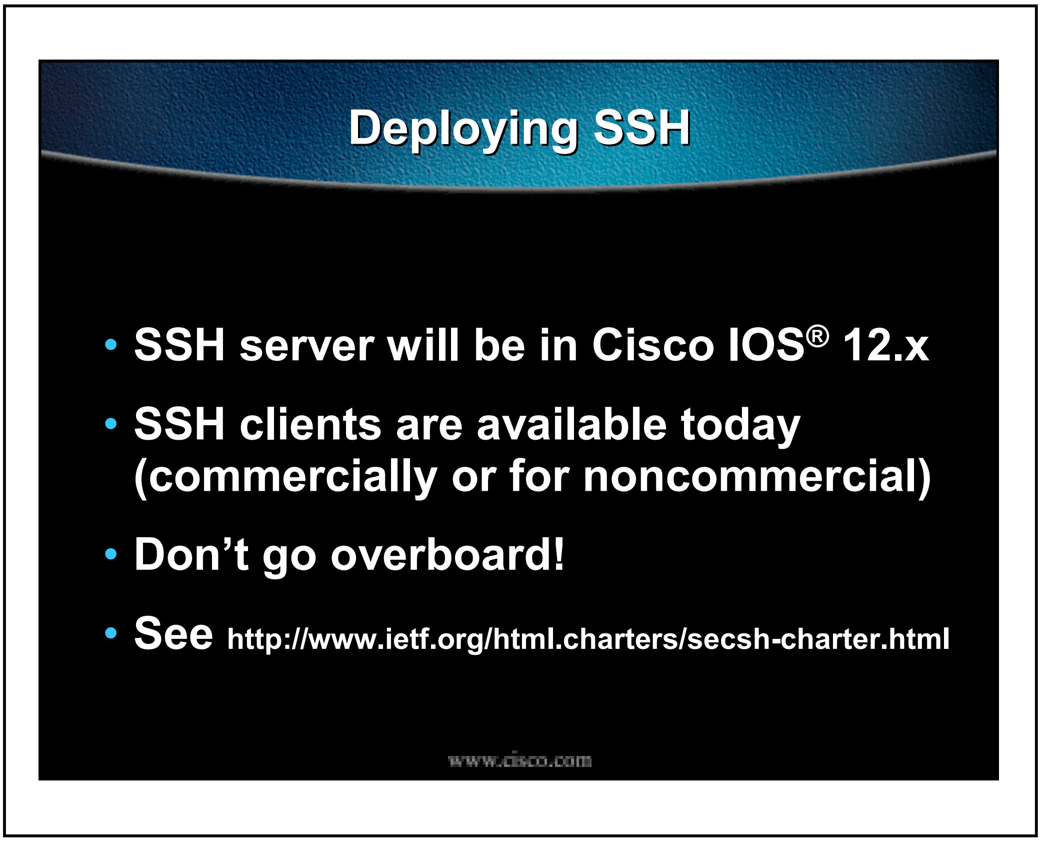
Public/Private Key Authentication

I dare You to say “Shazam”

Shazam! 1010101010098jlkf82189120j Shazam!

Shazam! X 870980jd09210982j092u0912 **Idiot!**

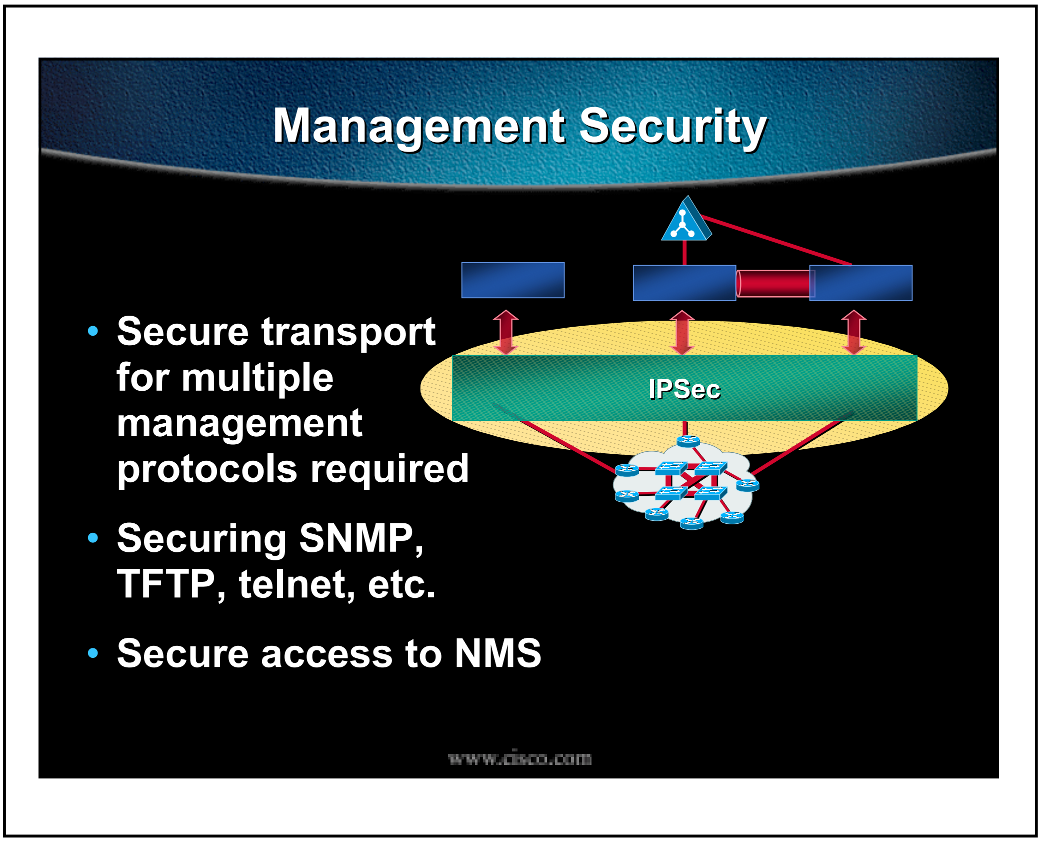
www.cisco.com



Deploying SSH

- SSH server will be in Cisco IOS® 12.x
- SSH clients are available today (commercially or for noncommercial)
- Don’t go overboard!
- See http://www.ietf.org/html.charters/secsh-charter.html

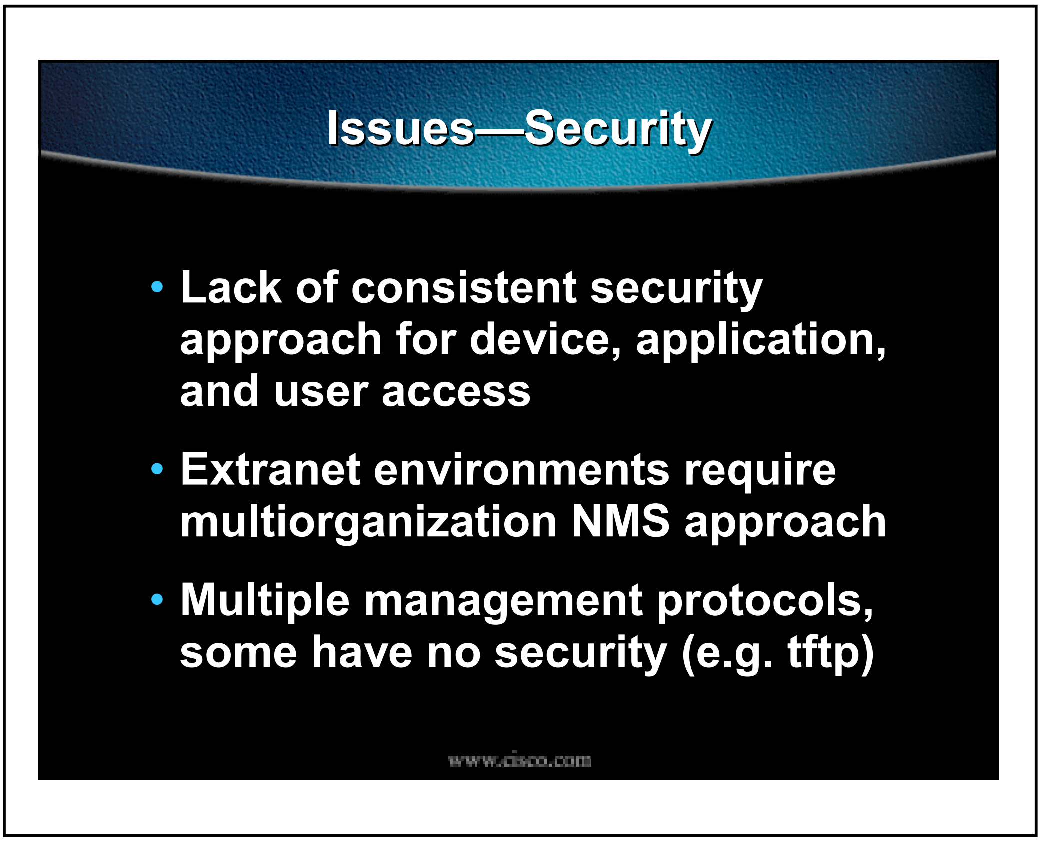
www.cisco.com



Management Security

- Secure transport for multiple management protocols required
- Securing SNMP, TFTP, telnet, etc.
- Secure access to NMS

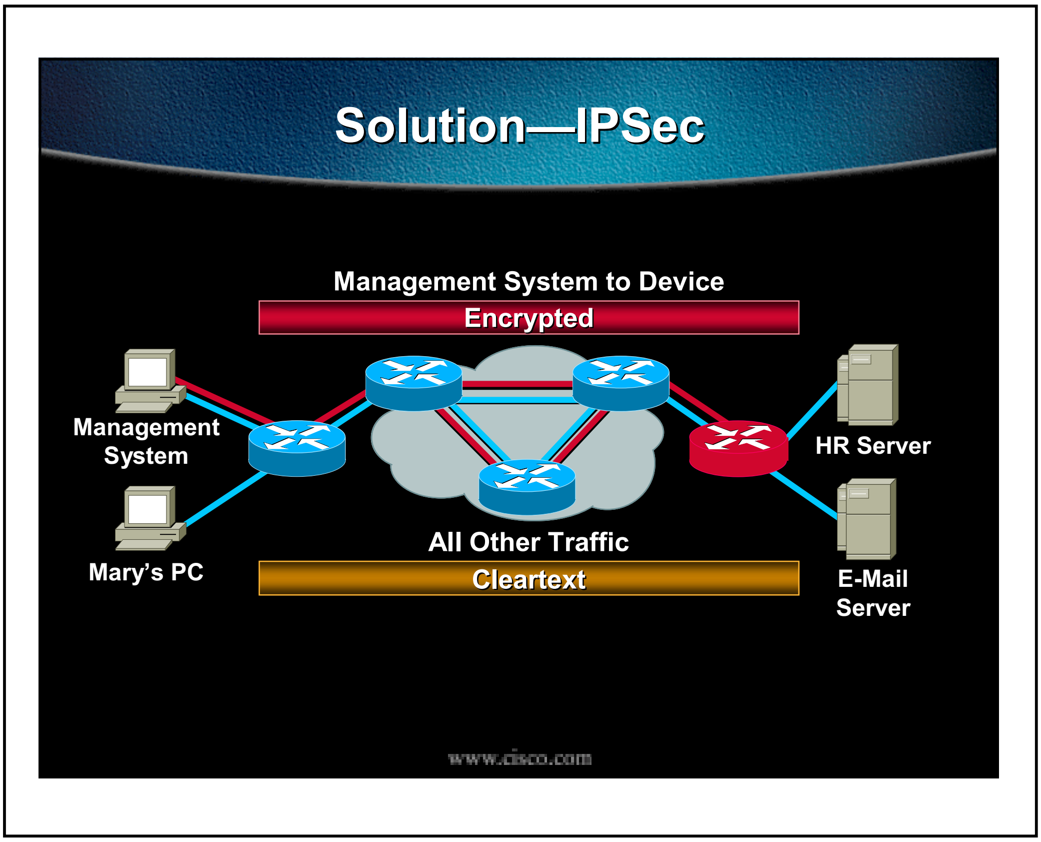
www.cisco.com



Issues—Security

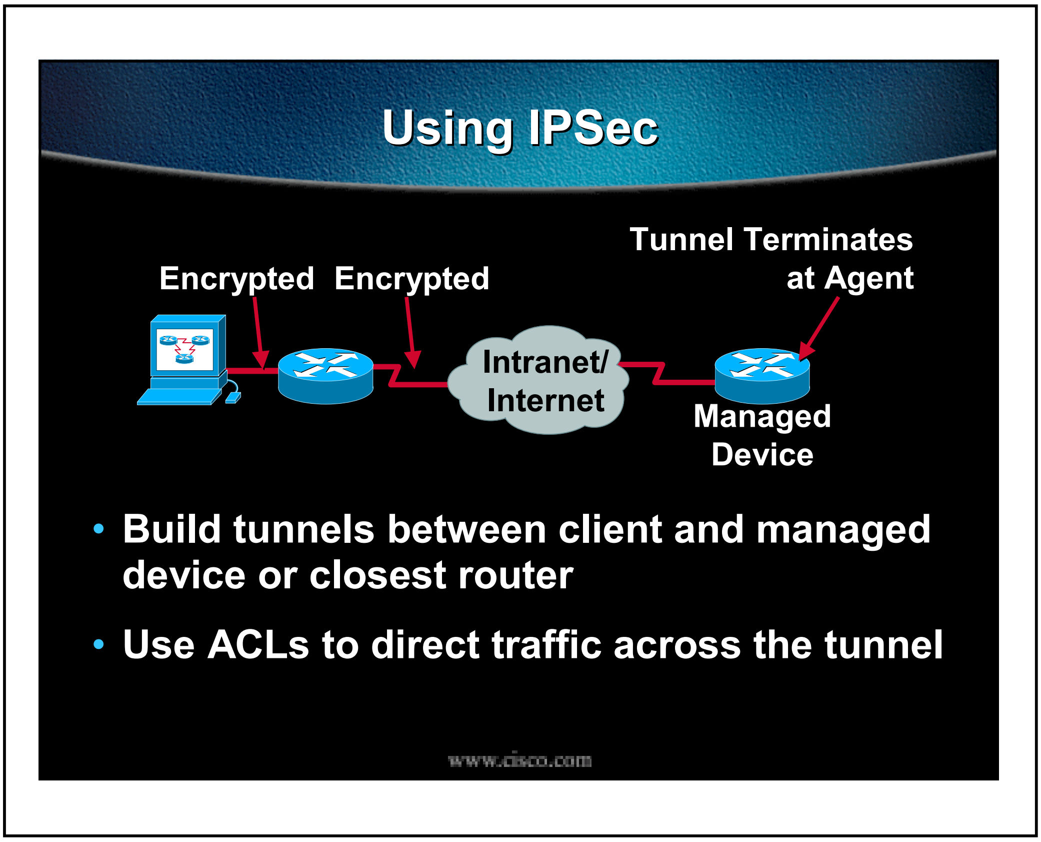
- Lack of consistent security approach for device, application, and user access
- Extranet environments require multiorganization NMS approach
- Multiple management protocols, some have no security (e.g. tftp)

www.cisco.com



Solution—IPSec

www.cisco.com



Using IPSec

Encrypted

Encrypted

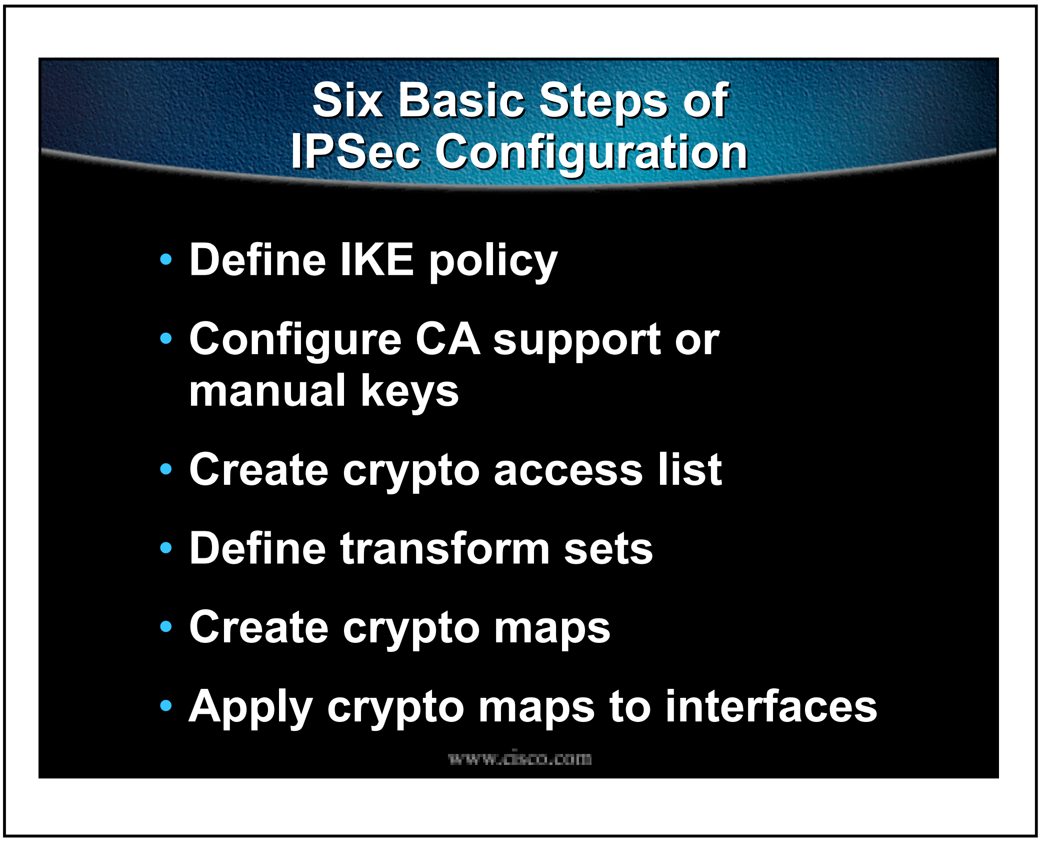
Tunnel Terminates at Agent

Intranet/ Internet

Managed Device

- Build tunnels between client and managed device or closest router
- Use ACLs to direct traffic across the tunnel

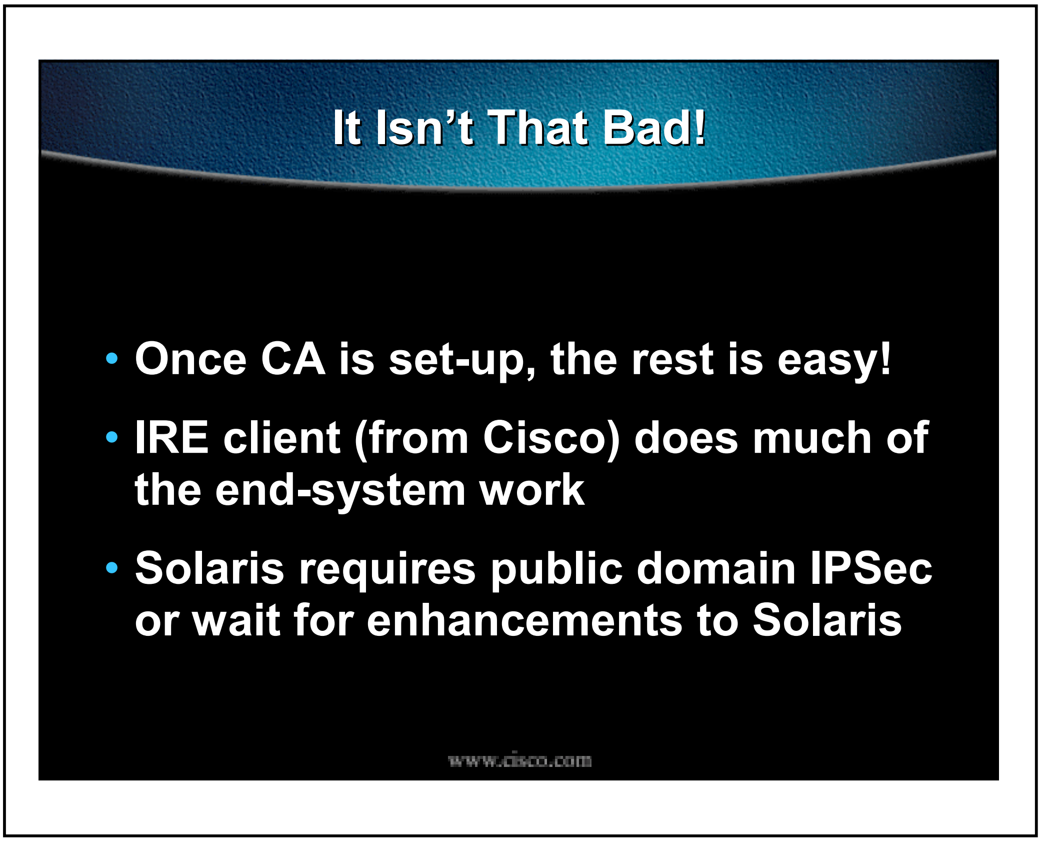
www.cisco.com



Six Basic Steps of IPSec Configuration

- Define IKE policy
- Configure CA support or manual keys
- Create crypto access list
- Define transform sets
- Create crypto maps
- Apply crypto maps to interfaces

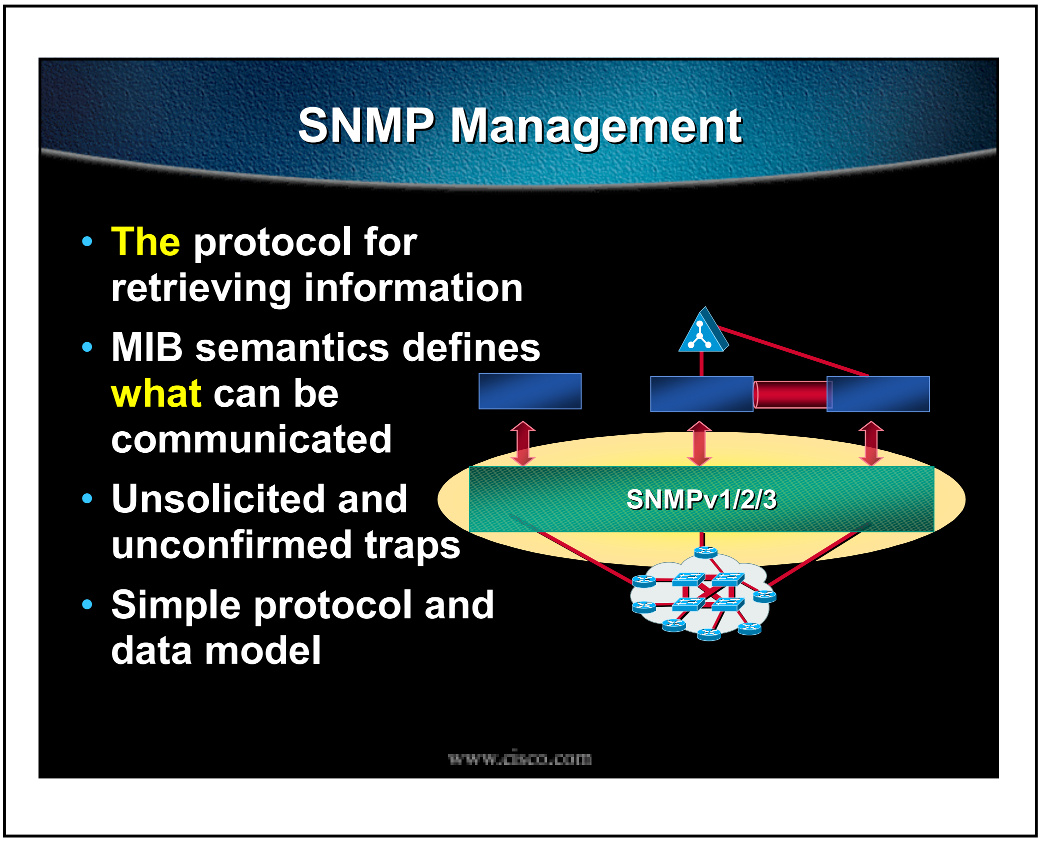
www.cisco.com



It Isn't That Bad!

- Once CA is set-up, the rest is easy!
- IRE client (from Cisco) does much of the end-system work
- Solaris requires public domain IPSec or wait for enhancements to Solaris

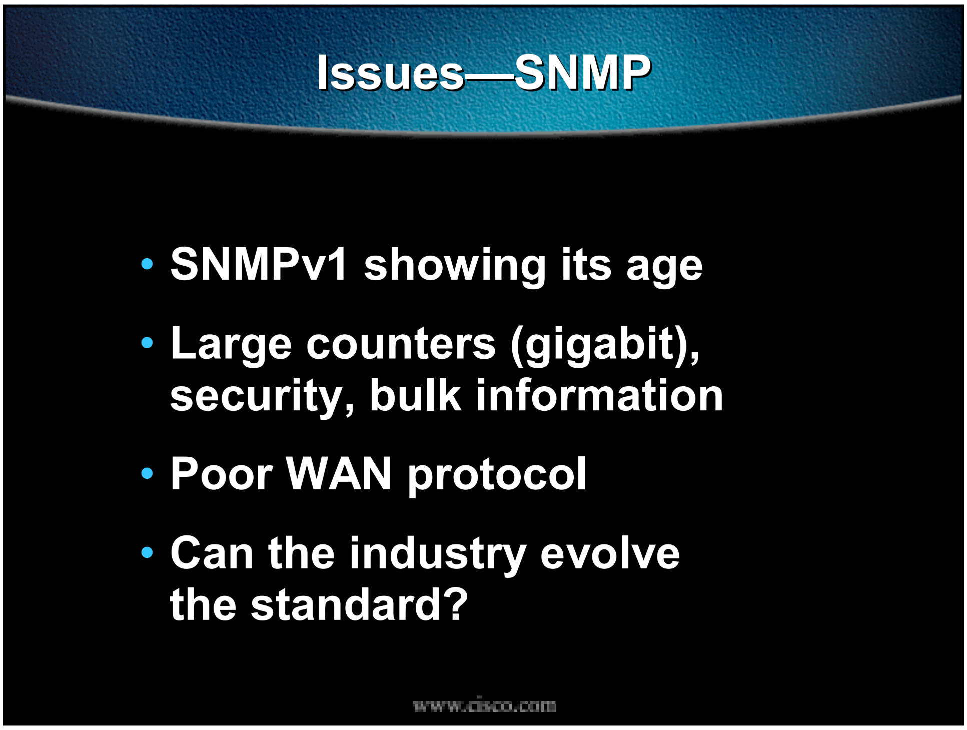
www.cisco.com



SNMP Management

- The protocol for retrieving information
- MIB semantics defines what can be communicated
- Unsolicited and unconfirmed traps
- Simple protocol and data model

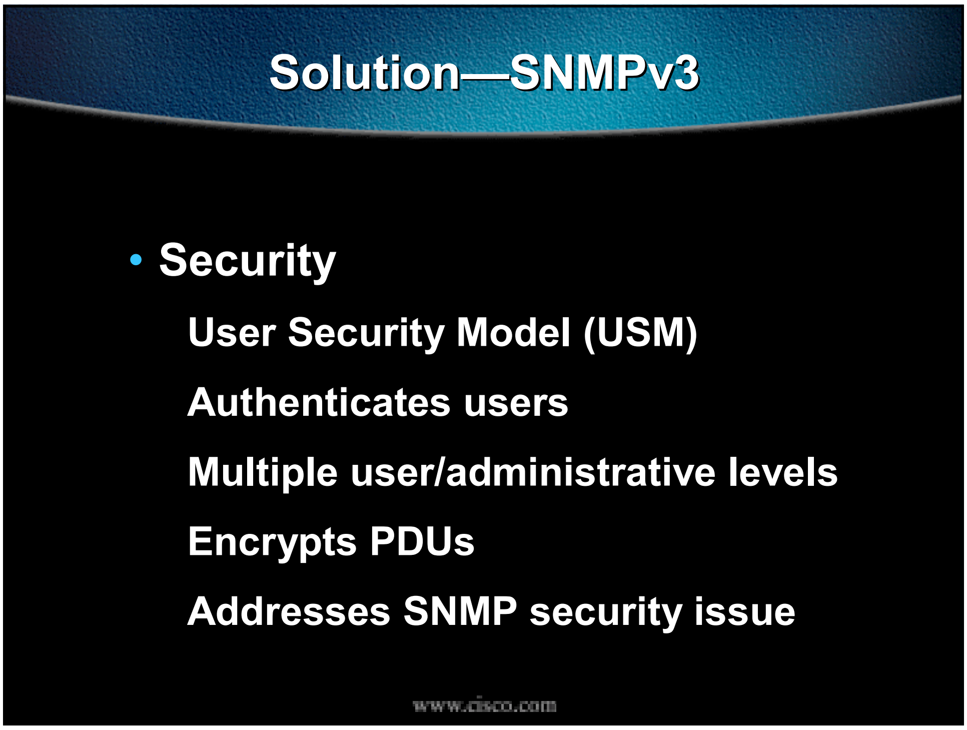
www.cisco.com



Issues—SNMP

- SNMPv1 showing its age
- Large counters (gigabit), security, bulk information
- Poor WAN protocol
- Can the industry evolve the standard?

www.cisco.com



Solution—SNMPv3

- Security

  User Security Model (USM)

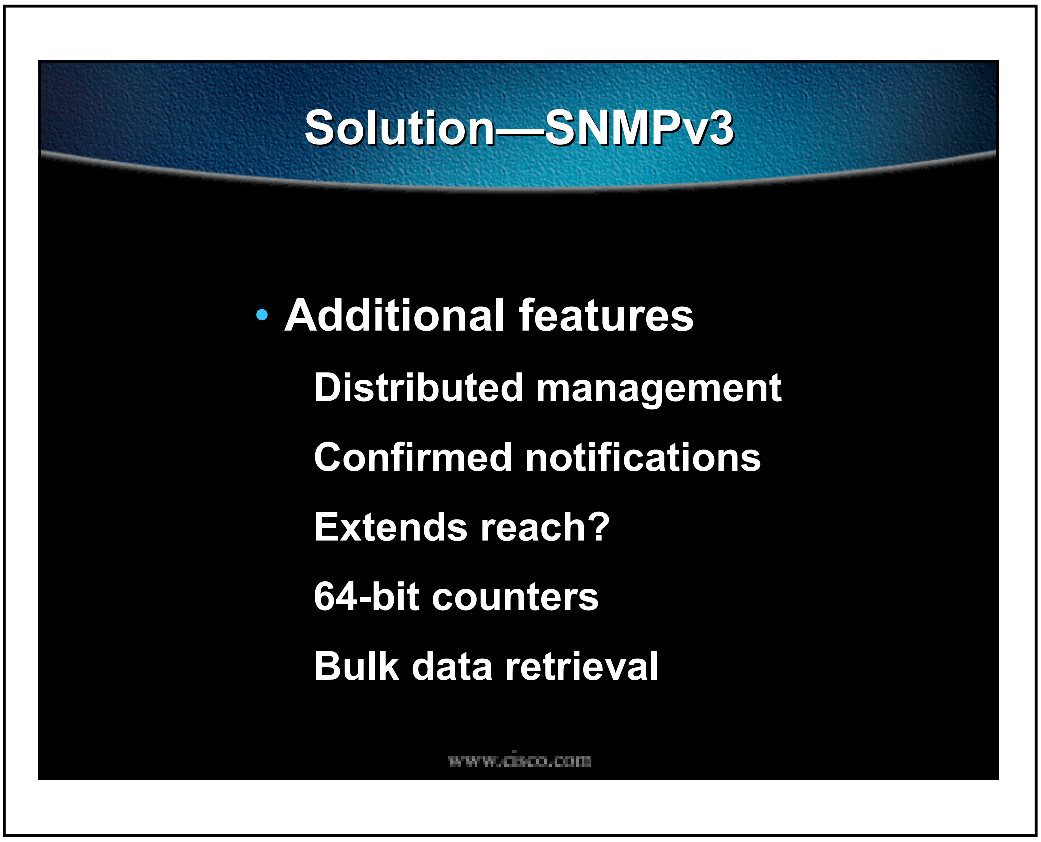
  Authenticates users

  Multiple user/administrative levels

  Encrypts PDUs

  Addresses SNMP security issue

www.cisco.com



Solution—SNMPv3

- Additional features

  Distributed management

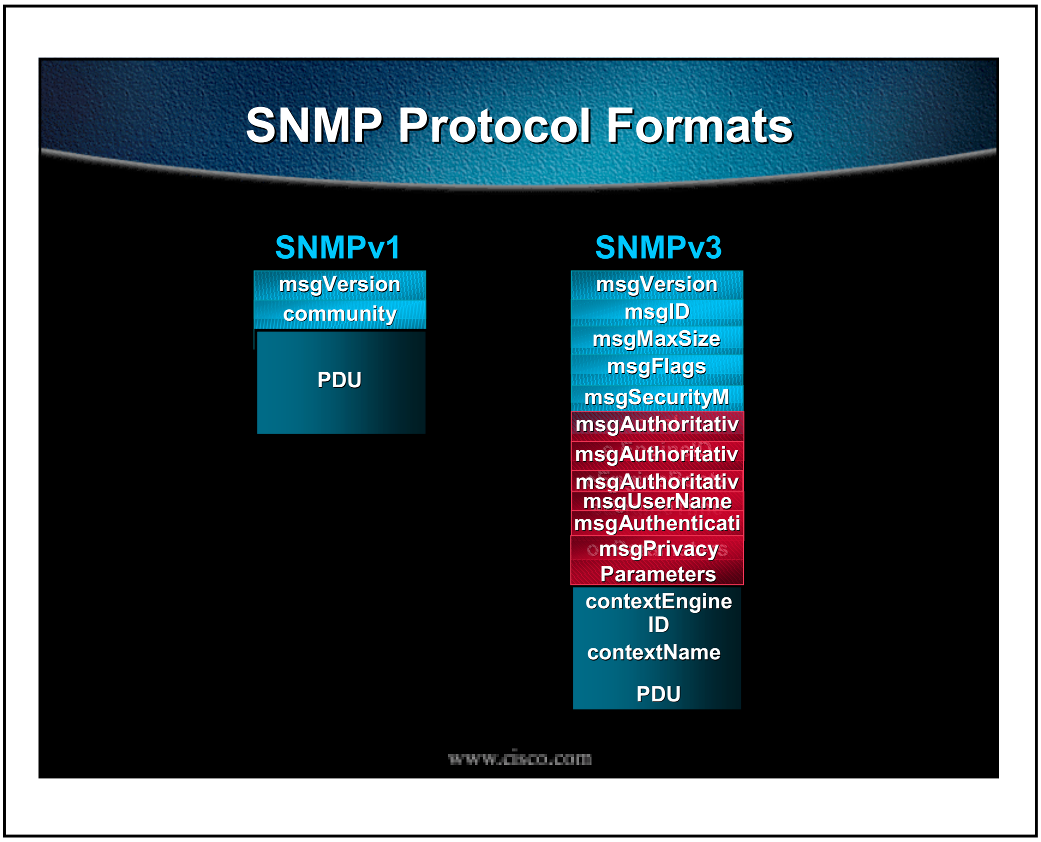
  Confirmed notifications

  Extends reach?

  64-bit counters

  Bulk data retrieval

www.cisco.com



SNMP Protocol Formats

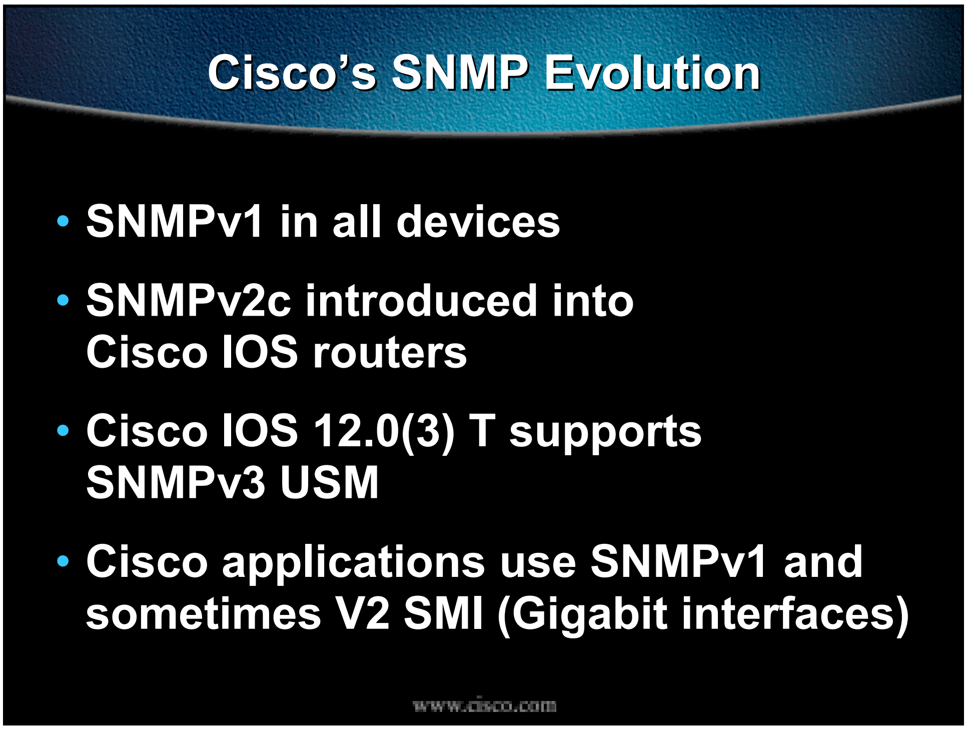
SNMPv1

msgVersion
community
PDU

SNMPv3

msgVersion
msgID
msgMaxSize
msgFlags
msgSecurityM
msgAuthoritativ
msgAuthoritativ
msgAuthoritativ
msgUserName
msgAuthenticati
msgPrivacy
Parameters
contextEngine
ID
contextName
PDU

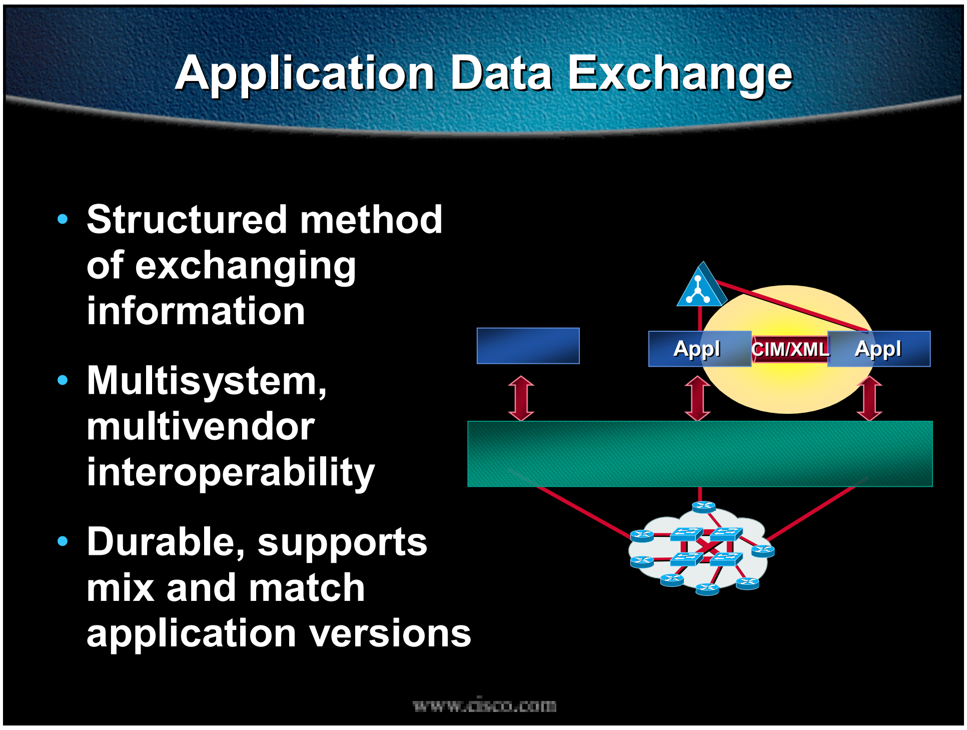
www.cisco.com



Cisco's SNMP Evolution

- SNMPv1 in all devices
- SNMPv2c introduced into Cisco IOS routers
- Cisco IOS 12.0(3) T supports SNMPv3 USM
- Cisco applications use SNMPv1 and sometimes V2 SMI (Gigabit interfaces)

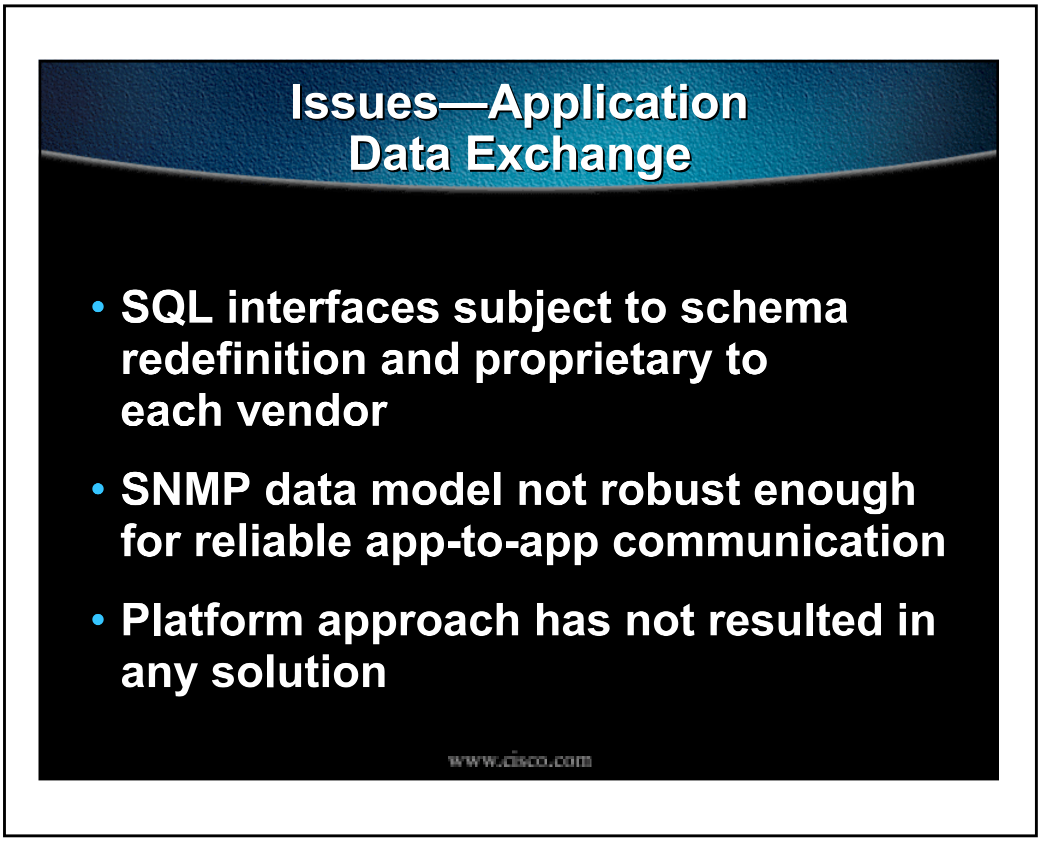
www.cisco.com



Application Data Exchange

- Structured method of exchanging information
- Multisystem, multivendor interoperability
- Durable, supports mix and match application versions

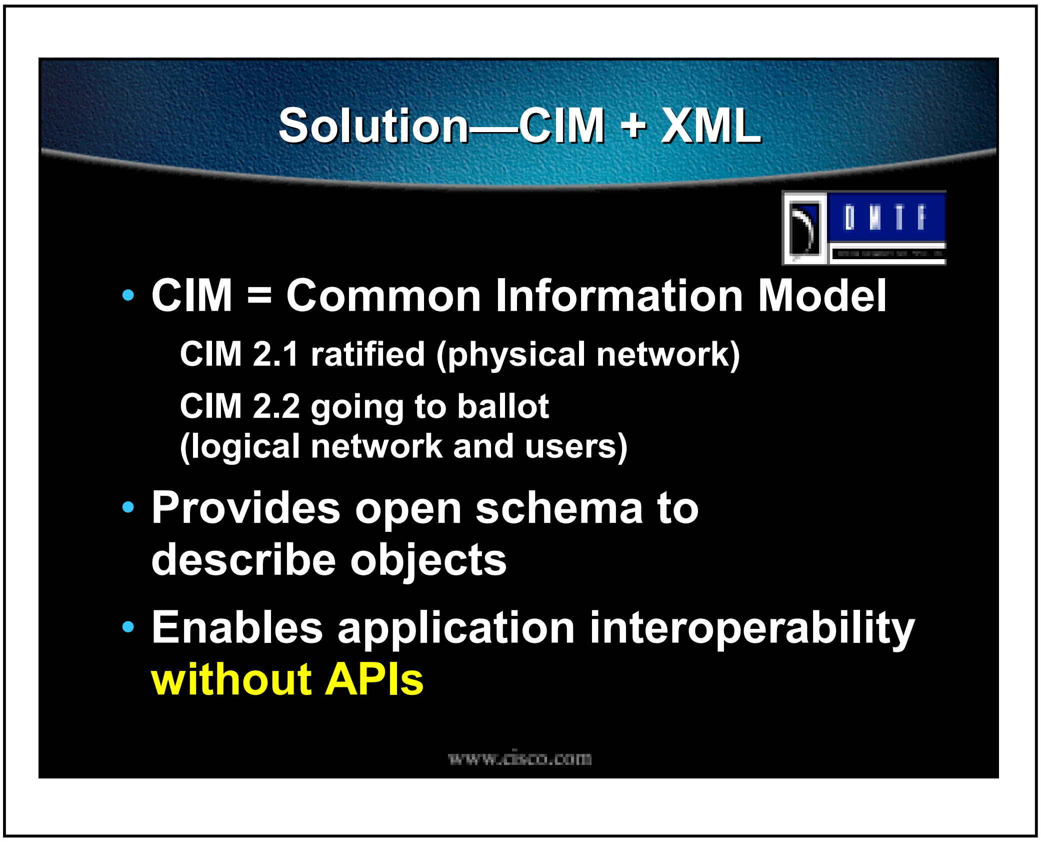
www.cisco.com



Issues—Application Data Exchange

- SQL interfaces subject to schema redefinition and proprietary to each vendor
- SNMP data model not robust enough for reliable app-to-app communication
- Platform approach has not resulted in any solution

www.cisco.com



Solution—CIM + XML

- CIM = Common Information Model

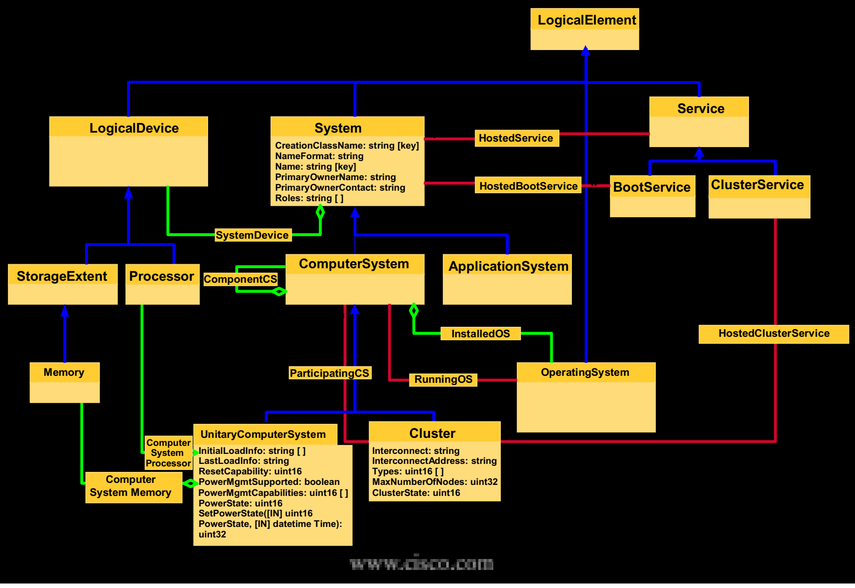
  CIM 2.1 ratified (physical network)

  CIM 2.2 going to ballot
  (logical network and users)

- Provides open schema to describe objects
- Enables application interoperability **without APIs**

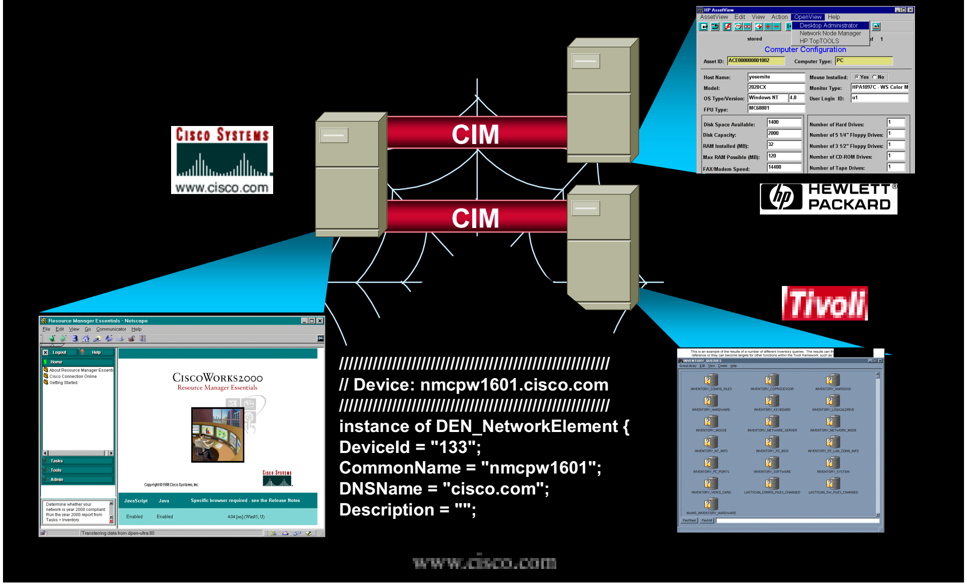
www.cisco.com

CIM Data Model



www.cisco.com

CIM Example: Inventory Data



Asset ID: ACE000000001002 Computer Type: PC

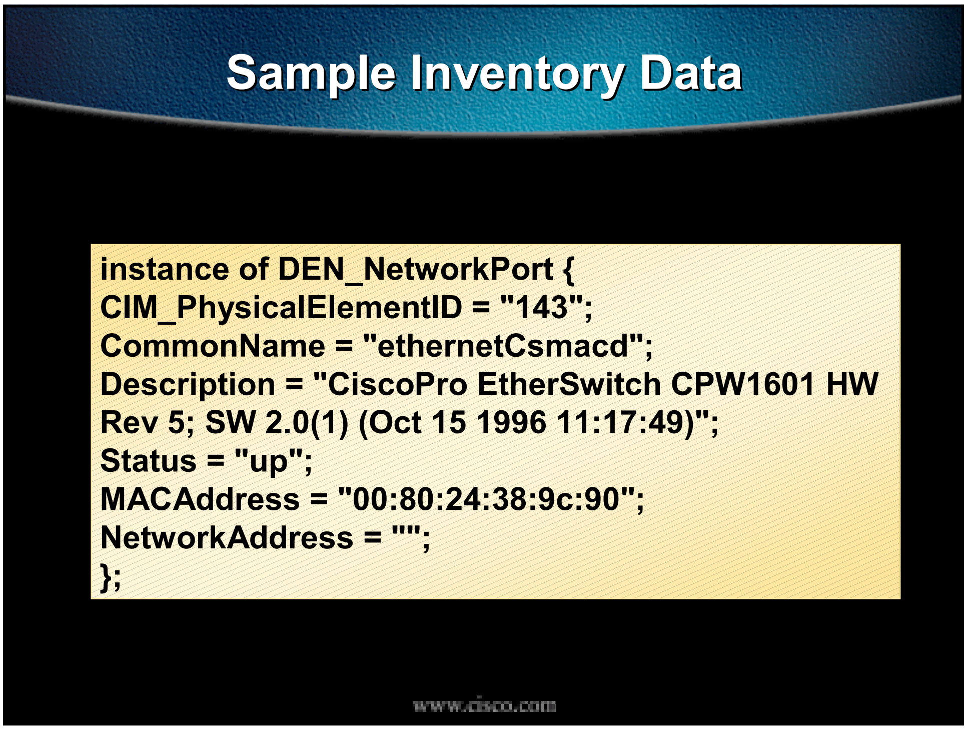
Host Name: yosemite
Model: 2020CX
OS Type/Version: Windows NT 4.0
FPU Type: MC68881
Mouse Installed: ● Yes ○ No
Monitor Type: HPA1097C - WS Color M
User Login ID: u1

Disk Space Available: 1400
Disk Capacity: 2000
RAM Installed (MB): 32
Max RAM Possible (MB): 120
FAX/Modem Speed: 14400

Number of Hard Drives: 1
Number of 5 1/4" Floppy Drives: 1
Number of 3 1/2" Floppy Drives: 1
Number of CD-ROM Drives: 1
Number of Tape Drives: 1

```
////////////////////////////////////////////////////////////
// Device: nmcpw1601.cisco.com
////////////////////////////////////////////////////////////
instance of DEN_NetworkElement {
DeviceId = "133";
CommonName = "nmcpw1601";
DNSName = "cisco.com";
Description = "";
```

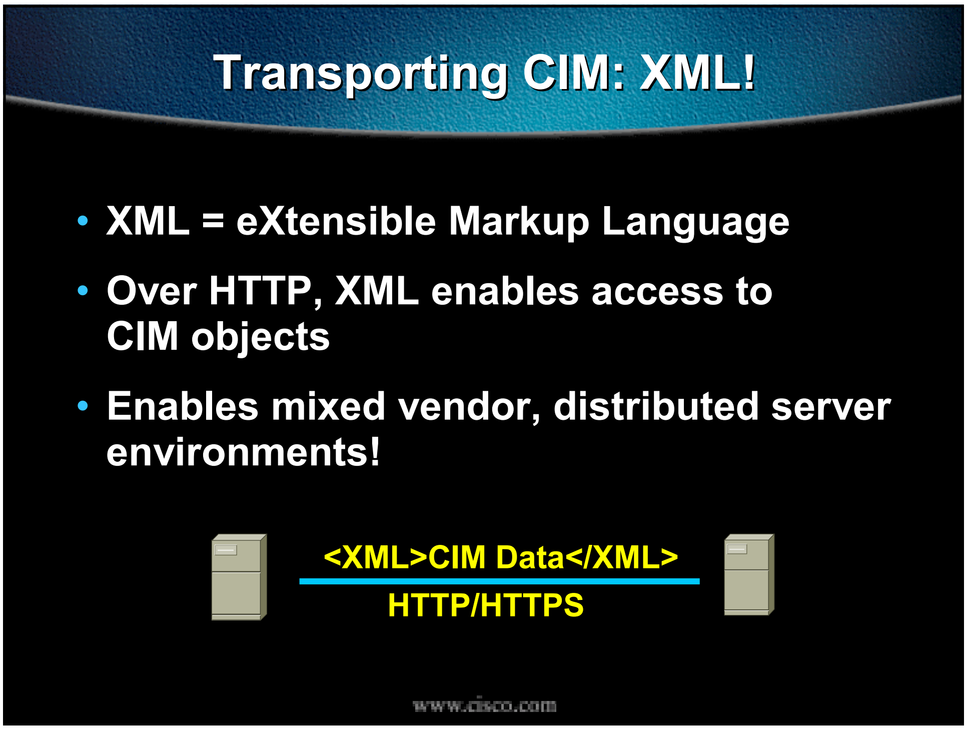
www.cisco.com



Sample Inventory Data

```
instance of DEN_NetworkPort {
CIM_PhysicalElementID = "143";
CommonName = "ethernetCsmacd";
Description = "CiscoPro EtherSwitch CPW1601 HW
Rev 5; SW 2.0(1) (Oct 15 1996 11:17:49)";
Status = "up";
MACAddress = "00:80:24:38:9c:90";
NetworkAddress = "";
};
```

www.cisco.com

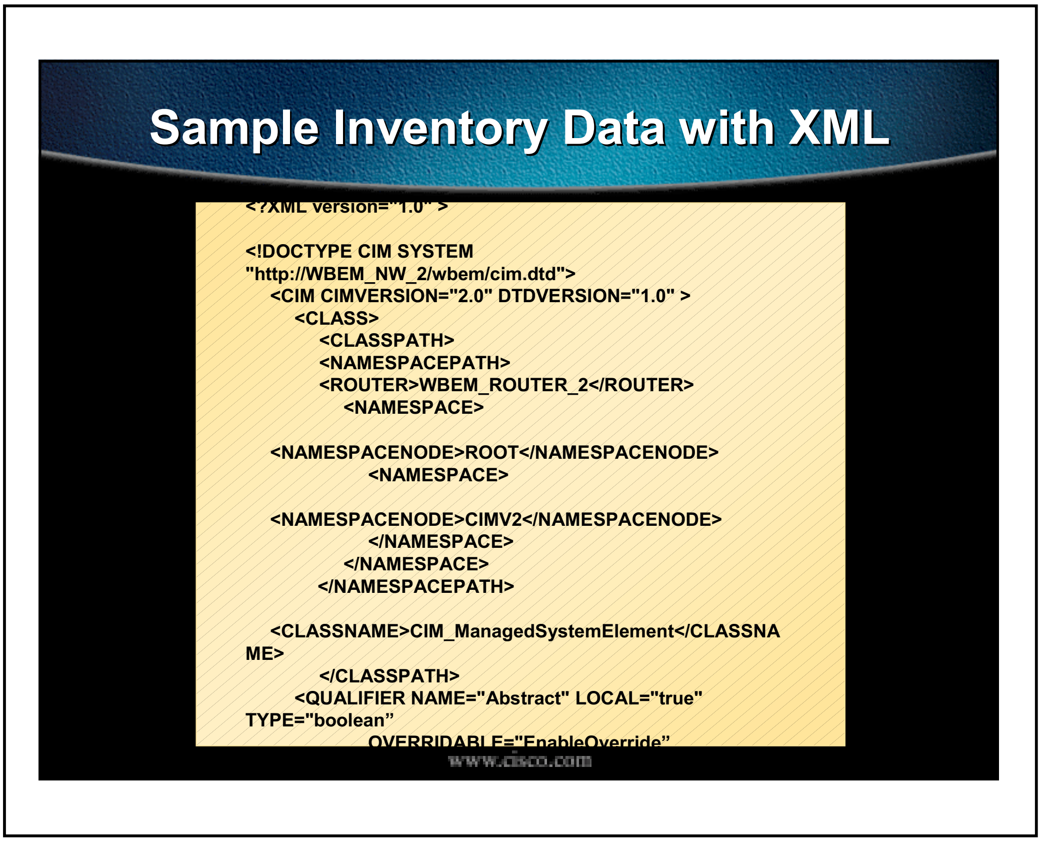


Transporting CIM: XML!

- XML = eXtensible Markup Language
- Over HTTP, XML enables access to CIM objects
- Enables mixed vendor, distributed server environments!

<XML>CIM Data</XML>
HTTP/HTTPS

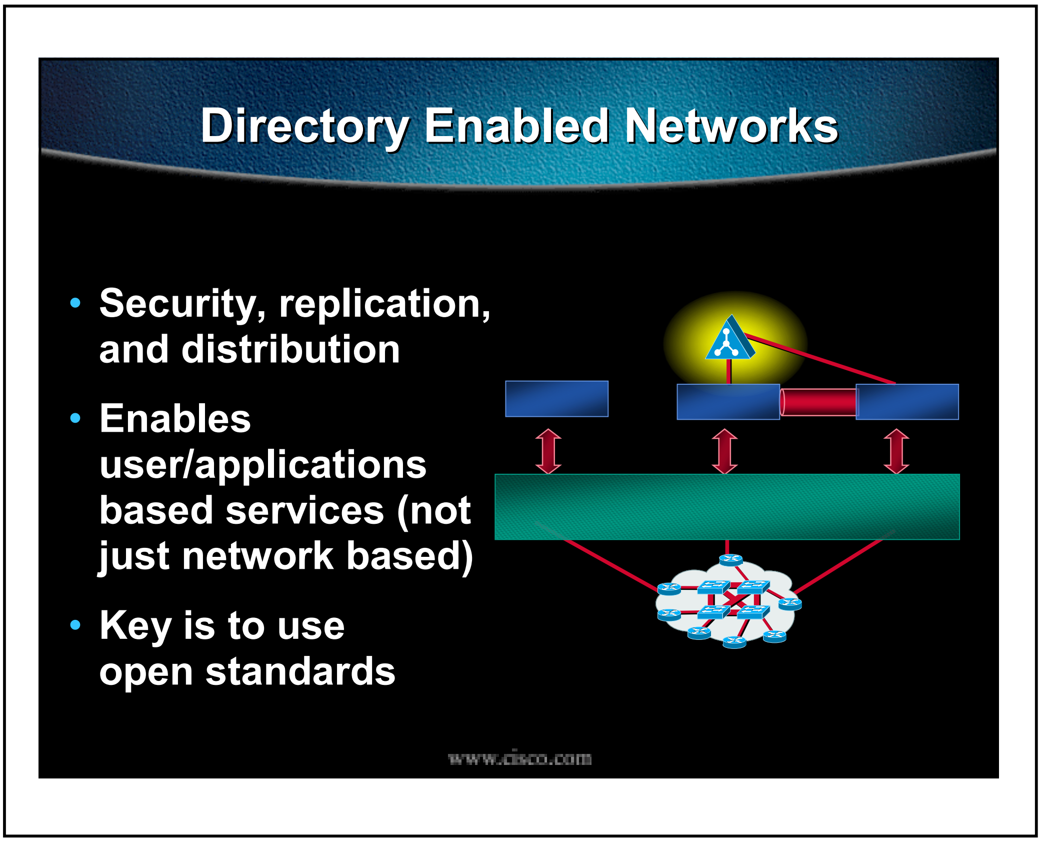
www.cisco.com



Sample Inventory Data with XML

```
<?XML version="1.0" >

<!DOCTYPE CIM SYSTEM
"http://WBEM_NW_2/wbem/cim.dtd">
    <CIM CIMVERSION="2.0" DTDVERSION="1.0" >
        <CLASS>
            <CLASSPATH>
            <NAMESPACEPATH>
            <ROUTER>WBEM_ROUTER_2</ROUTER>
                <NAMESPACE>

    <NAMESPACENODE>ROOT</NAMESPACENODE>
                    <NAMESPACE>

    <NAMESPACENODE>CIMV2</NAMESPACENODE>
                    </NAMESPACE>
                </NAMESPACE>
            </NAMESPACEPATH>

    <CLASSNAME>CIM_ManagedSystemElement</CLASSNA
ME>
            </CLASSPATH>
        <QUALIFIER NAME="Abstract" LOCAL="true"
TYPE="boolean”
                    OVERRIDABLE="EnableOverride”
```

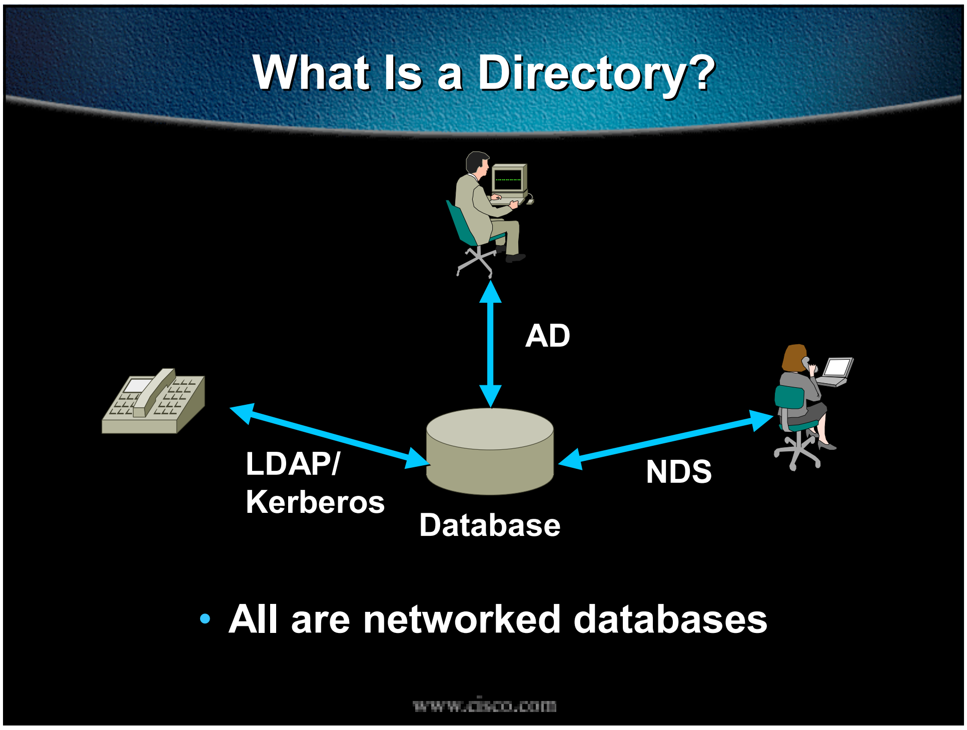
www.cisco.com



Directory Enabled Networks

- Security, replication, and distribution
- Enables user/applications based services (not just network based)
- Key is to use open standards

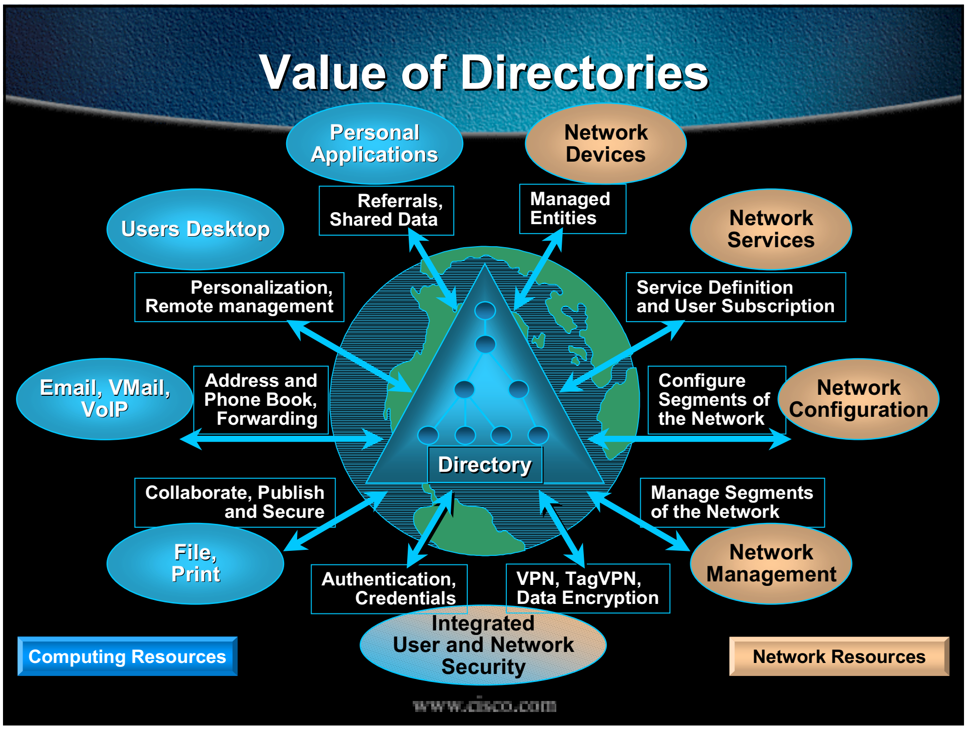
www.cisco.com



What Is a Directory?

- All are networked databases

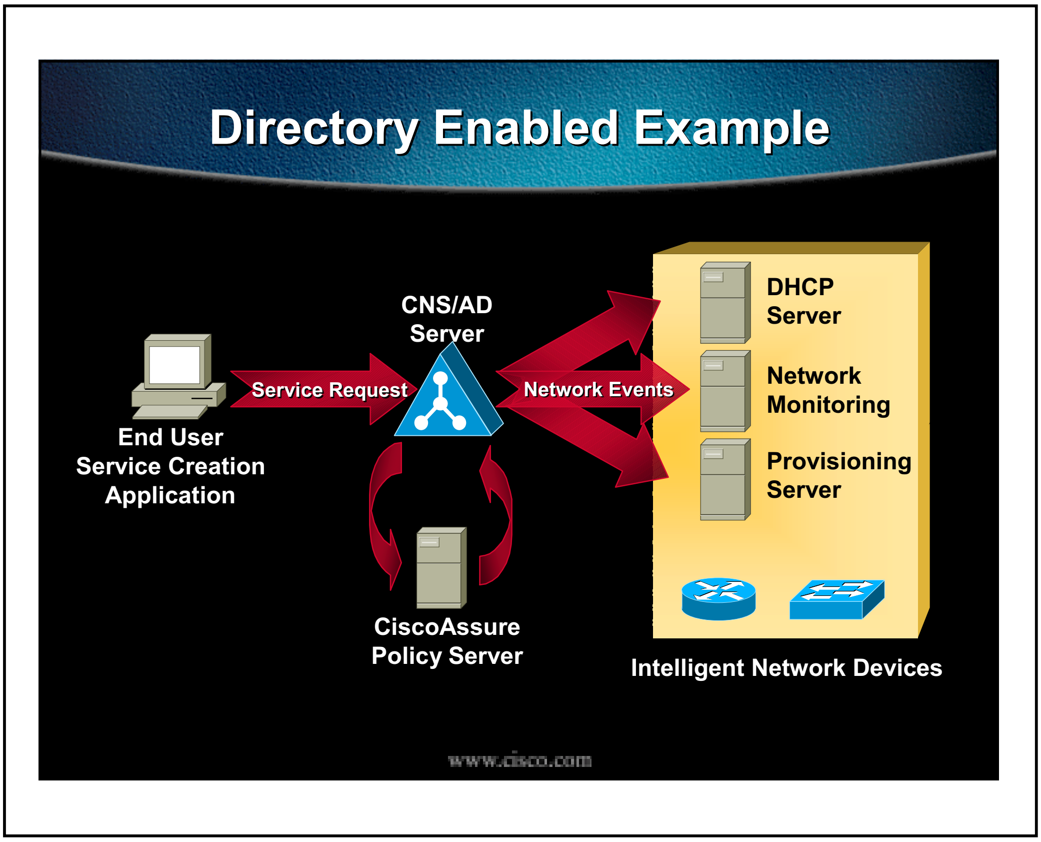
www.cisco.com



Value of Directories

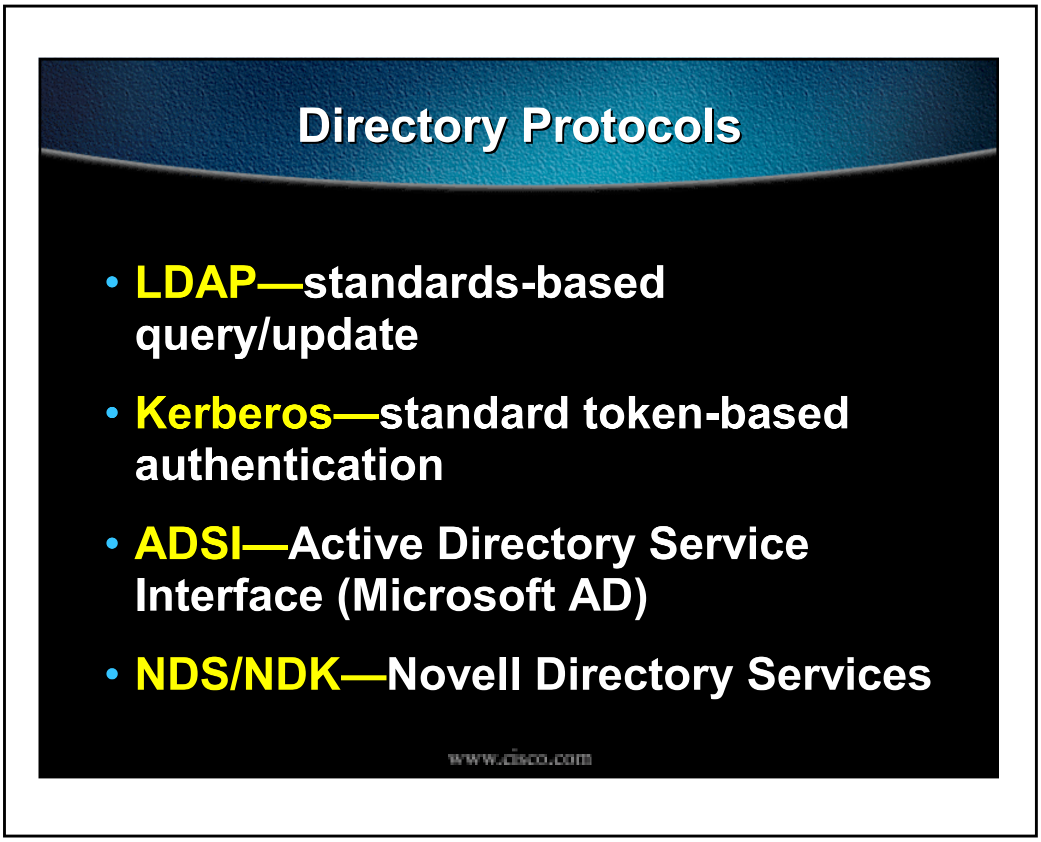
Personal Applications
Network Devices
Referrals, Shared Data
Managed Entities
Users Desktop
Network Services
Personalization, Remote management
Service Definition and User Subscription
Email, VMail, VoIP
Address and Phone Book, Forwarding
Configure Segments of the Network
Network Configuration
Directory
Collaborate, Publish and Secure
Manage Segments of the Network
File, Print
Network Management
Authentication, Credentials
VPN, TagVPN, Data Encryption
Integrated User and Network Security
Computing Resources
Network Resources

www.cisco.com



Directory Enabled Example

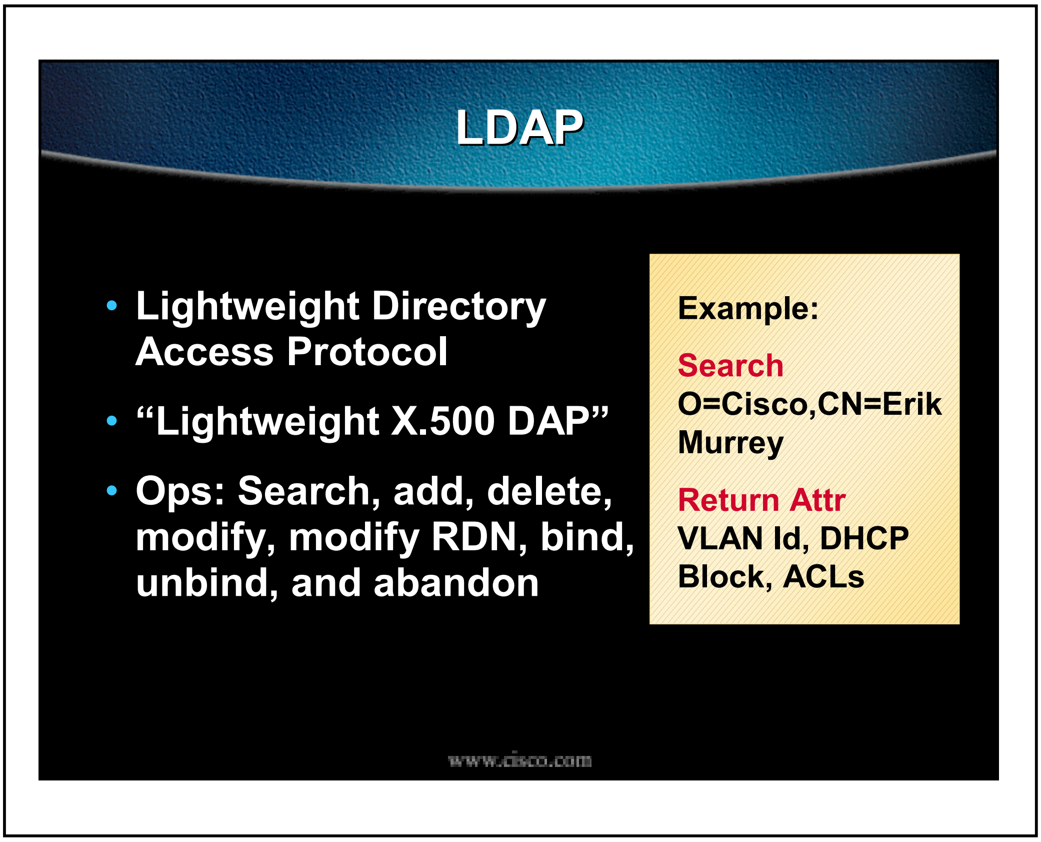
www.cisco.com



Directory Protocols

- **LDAP—**standards-based query/update
- **Kerberos—**standard token-based authentication
- **ADSI—**Active Directory Service Interface (Microsoft AD)
- **NDS/NDK—**Novell Directory Services

www.cisco.com



LDAP

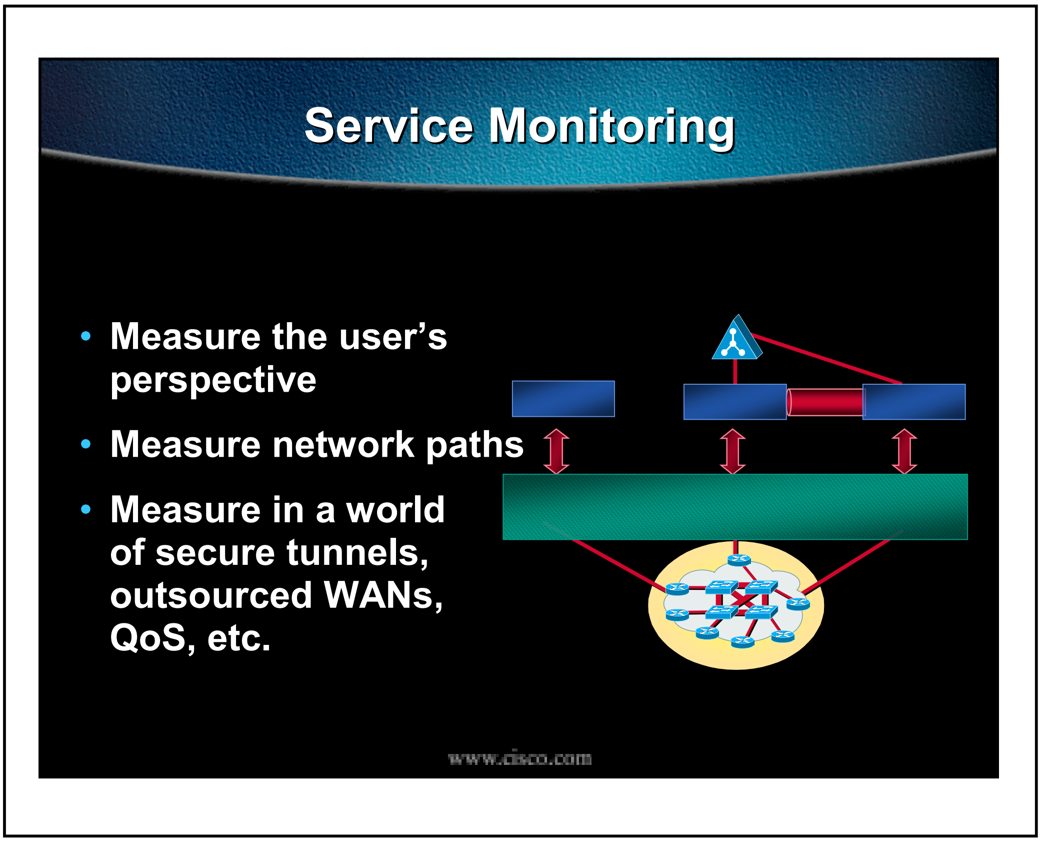
- Lightweight Directory Access Protocol
- “Lightweight X.500 DAP”
- Ops: Search, add, delete, modify, modify RDN, bind, unbind, and abandon

Example:

Search
O=Cisco,CN=Erik Murrey

Return Attr
VLAN Id, DHCP Block, ACLs

www.cisco.com



Service Monitoring

- Measure the user’s perspective
- Measure network paths
- Measure in a world of secure tunnels, outsourced WANs, QoS, etc.

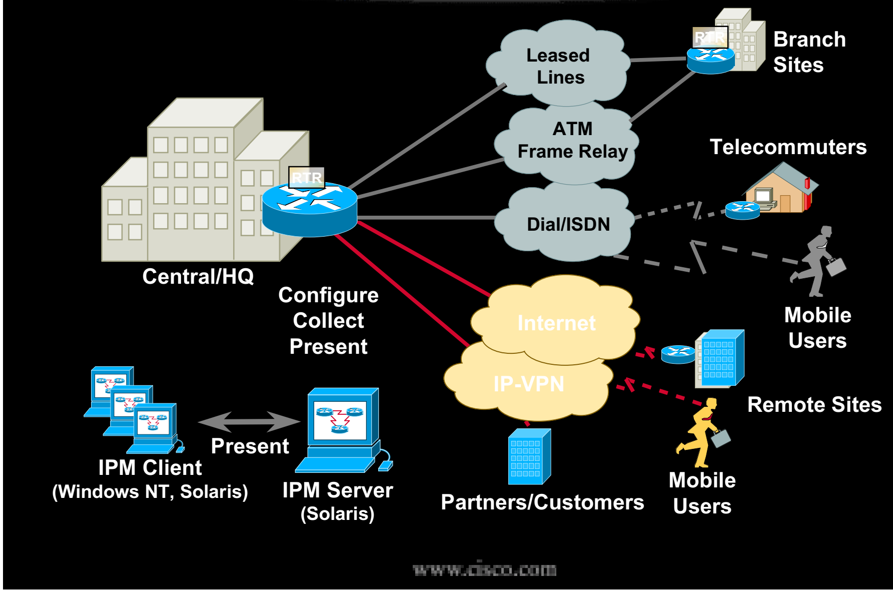
www.cisco.com

Issues—Service Monitoring

- Encryption of packets (IPSec) breaks probe/observation approach
- NMS “ping” approach
  - Doesn’t measure network paths
  - Can’t measure QoS enabled networks
- E-commerce, extranets, etc., require measurement of services and applications

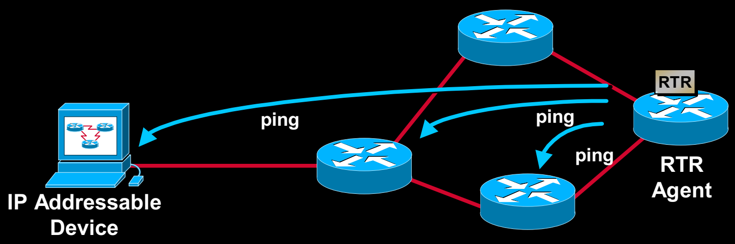
www.cisco.com

Solution—Network Based RTR



www.cisco.com

How RTR Works



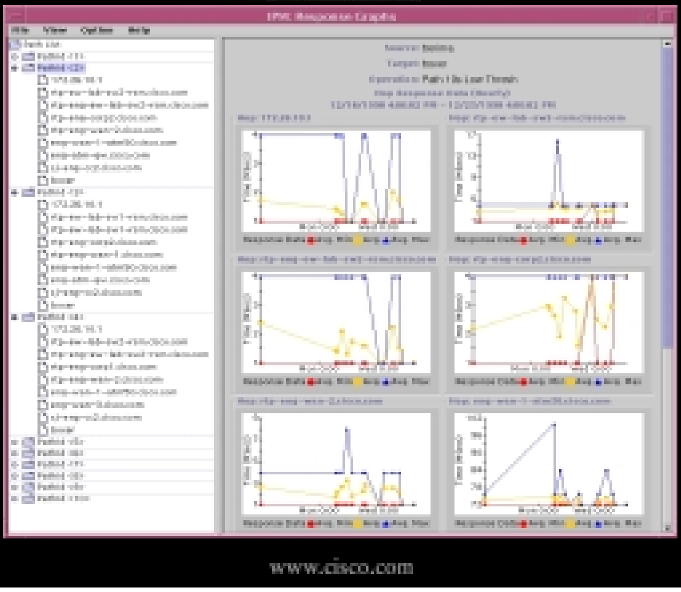
- Determine IP Path every measurement interval

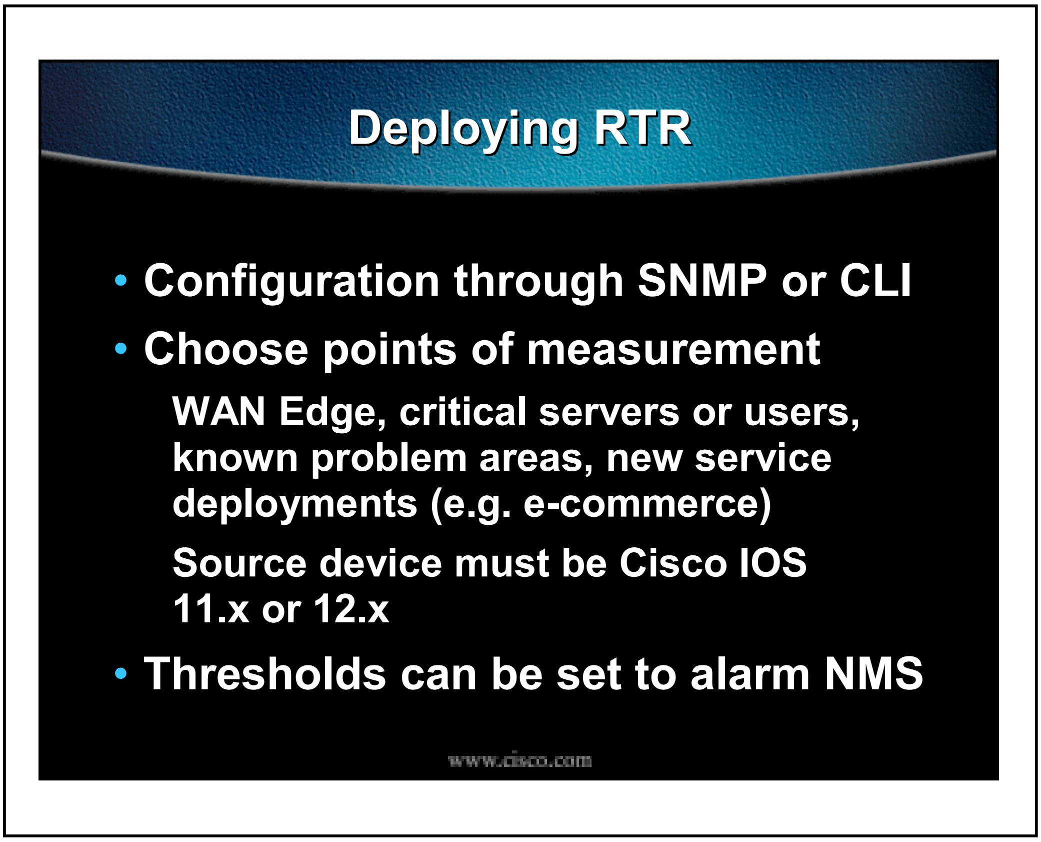
  Over time, discovers all active network paths

- Measure response time to each hop using ICMP, UDP, TCP-Connect, HTTP, DNS, VoIP

- Isolates hop that causes a SLA violation

Example Hop-by-Hop Report





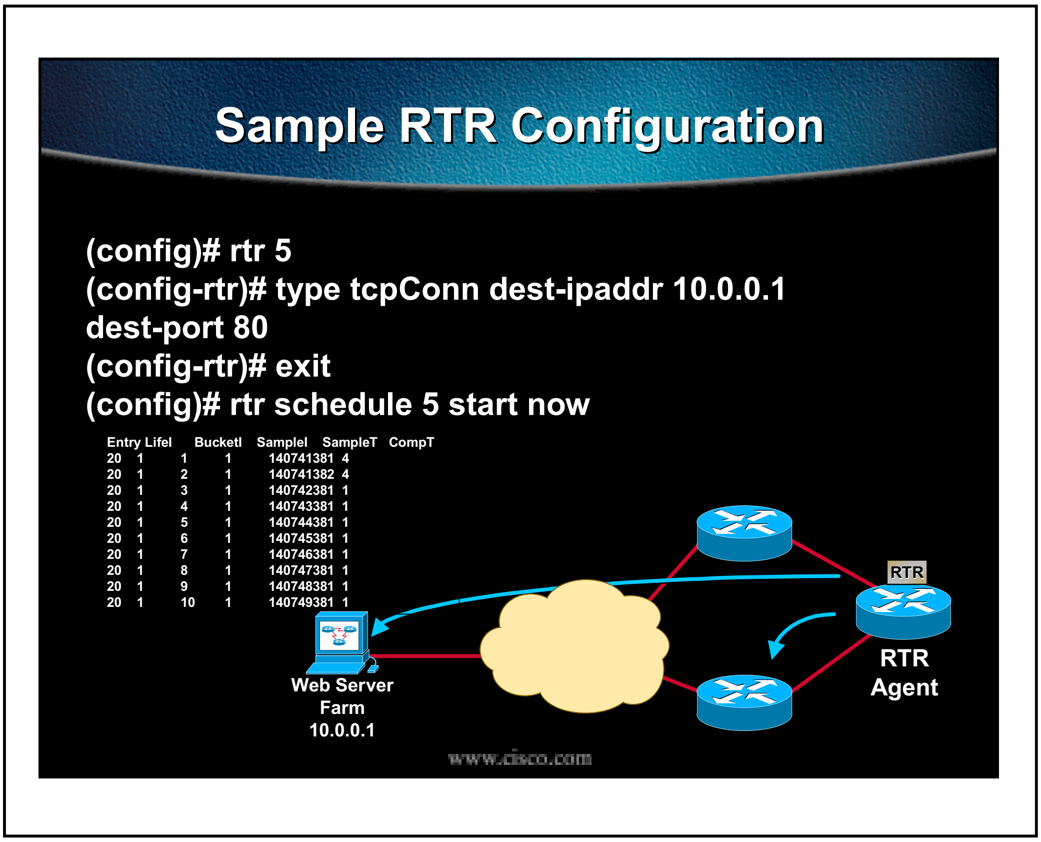
Deploying RTR

- Configuration through SNMP or CLI
- Choose points of measurement

  WAN Edge, critical servers or users, known problem areas, new service deployments (e.g. e-commerce)

  Source device must be Cisco IOS 11.x or 12.x
- Thresholds can be set to alarm NMS

www.cisco.com

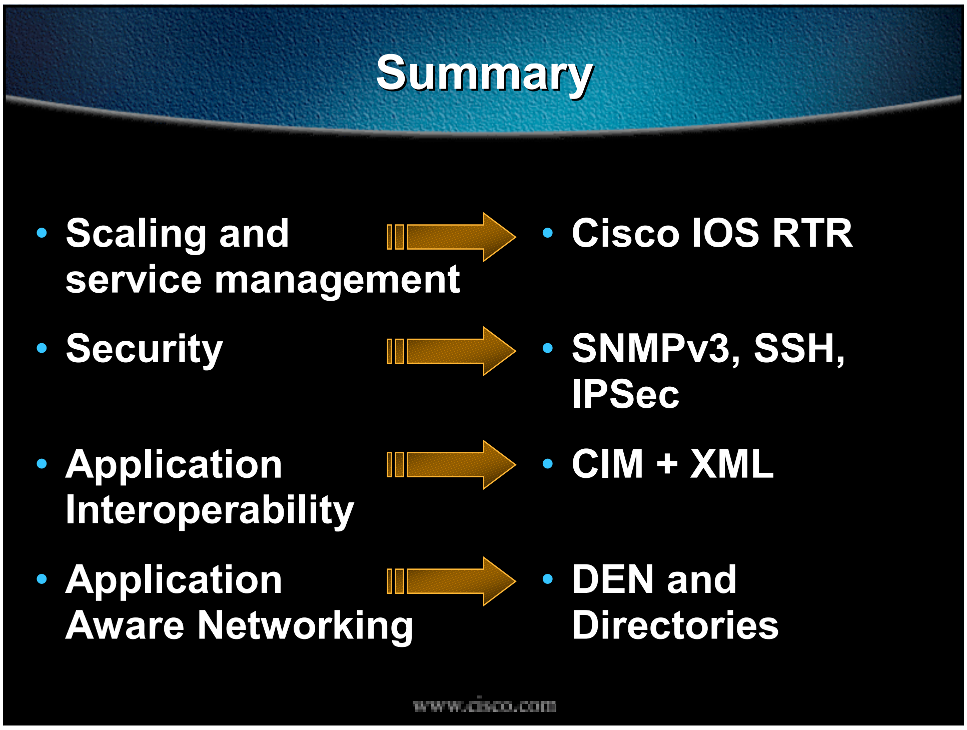


Sample RTR Configuration

```
(config)# rtr 5
(config-rtr)# type tcpConn dest-ipaddr 10.0.0.1
dest-port 80
(config-rtr)# exit
(config)# rtr schedule 5 start now
```

```
Entry Lifel    BucketI   SampleI   SampleT   CompT
20   1     1       1      140741381  4
20   1     2       1      140741382  4
20   1     3       1      140742381  1
20   1     4       1      140743381  1
20   1     5       1      140744381  1
20   1     6       1      140745381  1
20   1     7       1      140746381  1
20   1     8       1      140747381  1
20   1     9       1      140748381  1
20   1     10      1      140749381  1
```

www.cisco.com



Summary

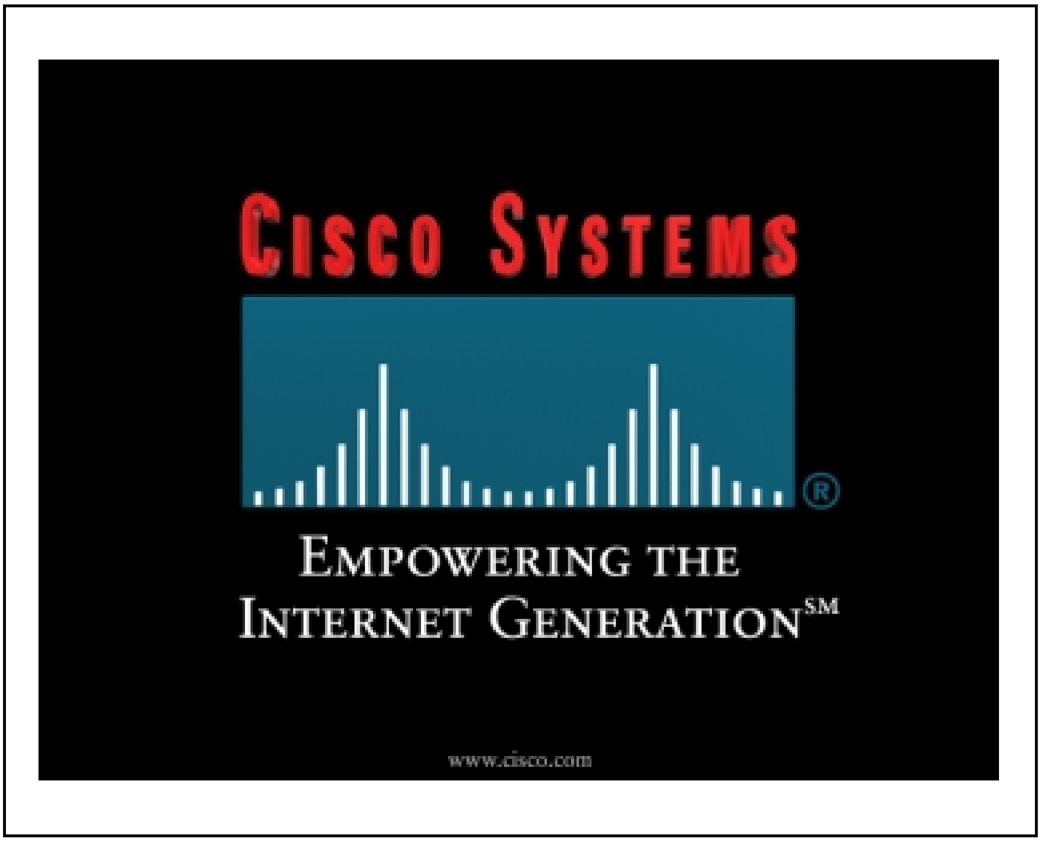
- Scaling and service management → Cisco IOS RTR
- Security → SNMPv3, SSH, IPSec
- Application Interoperability → CIM + XML
- Application Aware Networking → DEN and Directories

www.cisco.com

Please Complete Your Evaluation Form

Session 801

www.cisco.com



Cisco Systems®

Empowering the
Internet Generation℠

www.cisco.com