

Cisco IOS Software in the Telco Data Communications Network

Abstract

Strategies are being put in place by telcos and large facilities-based service providers whose aim it is to build the “network of networks” for the Telecommunications Management Network’s (TMN’s) data communications network (DCN). The underlying goal of such a network is multifold: to consolidate networking resources, resulting in an reduction in operating costs; to turn up new revenue-generating services faster; and to scale to meet the rapid growth of data equipment deployment such as SONET/SDH and DSL gear. The discussion in this paper refers to telcos (ILECs and PTTs) and large facilities-based service providers (IXCs, cable operators, wireless). This is the primary DCN market. However, the subject matter applies equally well to the secondary market of smaller facilities-based service providers such as CLECs (competitive local exchange carriers), NLOs (new licensed operators), independent operating companies (IOCs), and alternate carriers.

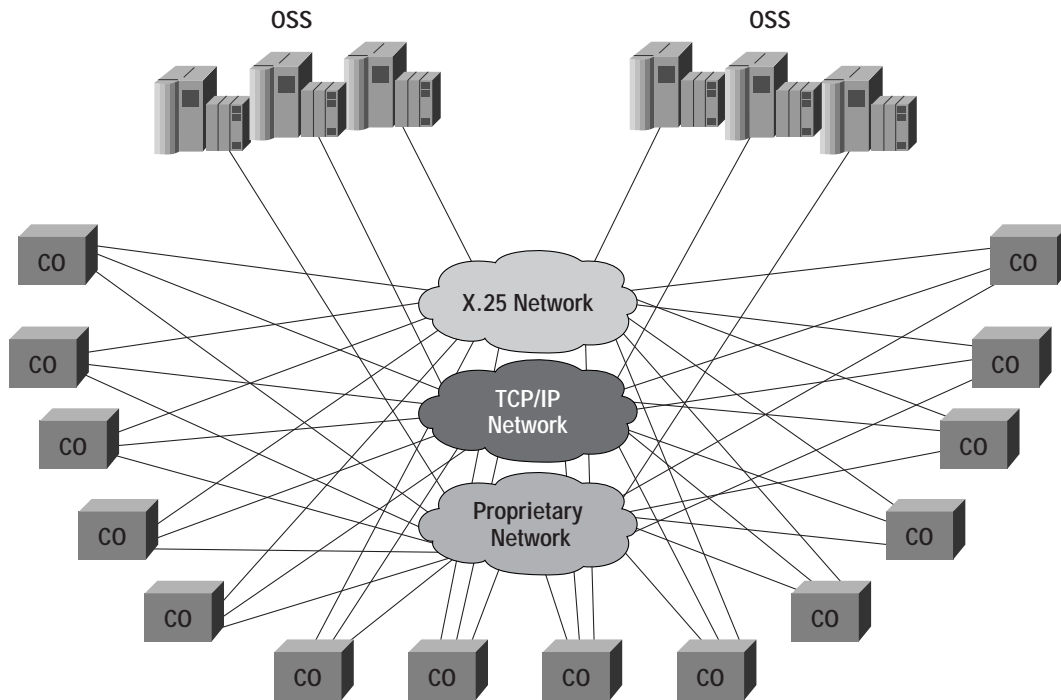
The DCN is used in the management of all network elements in the central office including the voice networking components, SONET/SDH equipment and digital cross-connect systems. In today’s rapidly changing networking environment, a DCN solution must be more scalable, adaptable, and provide greater interconnectivity and be standards-based in order to comply with the evolving business requirements of service providers. Since there are many disparate data networks within the current DCN architecture, this paper will discuss the telco DCN environment as it pertains to the objectives of the TMN. It also identifies obstacles that the DCN must overcome to positively affect the telco bottom line by being efficient and responsive to the demands placed upon it. DCN network planners are implementing strategies that only consider vendors with well-thought-out and well-designed end-to-end solutions to help them create the “network of networks”. Niche players who only provide point solutions will be used less frequently. Cisco IOS[®] software will play an integral part by providing the scalable end to end solution for the telco DCN of the future.

The Telco DCN

If one were to dissect the telephone company (telco) network, one would examine the telco’s distributed locations, called central offices (CO) or points of presence (POP). There, we would find a world of copper, fiber, cables, interfaces, transmission systems, voice and data switching systems, multiplexers, digital cross connect systems (DCS), signaling terminals, front-end processors, mainframes, cluster controllers, file servers, and so on. In general, the intelligent components are referred to as network elements (NE), which are connected directly or indirectly to the networks voice backbone that transports our calls.

All NEs need to be managed from a centralized operations support system (OSS) located in one of several telco network operation centers (NOC). NEs have hardware interfaces used for management purposes such as retrieval of diagnostics, statistics, alarms, and provisioning. These management interfaces communicate to the OSS via some form of protocol over a network called the DCN. Unfortunately, the NE components do not communicate using the same protocol, and they are a major reason for so many overlay management networks or DCNs (Figure 1) being deployed in the telco over the past several decades.

Figure 1 Overlapping Disparate DCNs



These multiple DCNs require that the Telco carry a significant financial burden since, in many cases, each network supports a dissimilar WAN protocol such as BX.25, X.25, IP, OSI, and others. There are many years of investment in legacy NEs whose interfaces do not, nor will they ever, migrate to a common protocol such as IP. By collapsing the various networks on to one “network of networks”, telcos could potentially save hundreds of thousands of dollars per year, per central office. This savings is realized by no longer having to purchase nor maintain CSU/DSUs, backbone components, network management platforms, recurring trunk access line costs and the ability to redeploy some of the network management personnel since the other overlay networks are no longer required.

TMN in the DCN

DCN is an out-of-band network that usually does not traverse the voice/user data network that it helps manage. The DCN is part of the Telecommunications Management Network (TMN) as defined by ITU-T specification M.3010. This recommendation defines the management requirements of administrations to plan, provision, install, maintain, operate and administer telecommunications networks and services. It provides management functions for telecommunication networks and services, offering communications between itself and the telecommunication networks, services, and other TMNs

The DCN network consists of many different types of devices that, in many cases, have different management interface protocols, hence, different networks. One will find that this spectrum of standards-based, and, in some instances, proprietary, protocols enables niche network hardware providers to create their individual markets. This is one of the obstacles, which prohibits the DCN network implementers from building their ultimate vision of the “network of networks”.

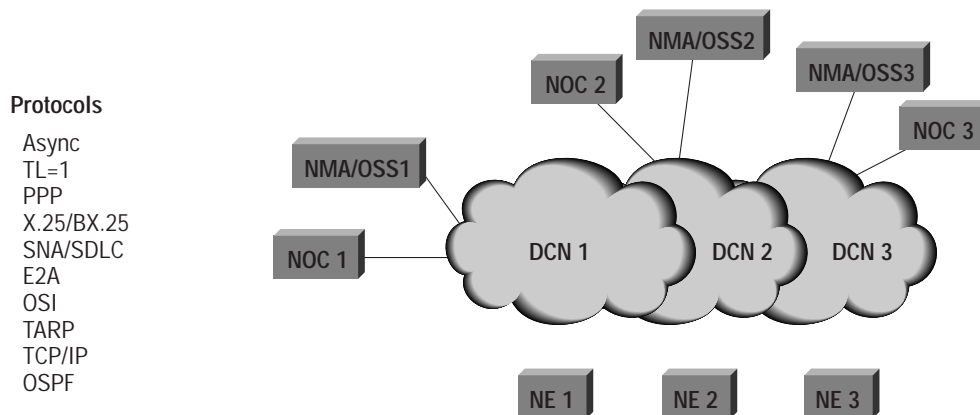
Description of Today's Telco Solutions

The majority of DCNs or their individual components still have diagnostic or management interfaces that are based on a very mature technology called X.25 which is still an CCITT/ITU-T recommendation. This technology is the glue that connects the network monitoring system application host to the various network elements (NEs) in the central office. Traditionally, access to these NEs is via X.25, BX.25 or asynchronously connected X.3 PADs. Because of CPU technology available in the 1970s, X.25 backbone or access link speeds were artificially maximized at 56kb. This limitation was viewed as one of the bottlenecks of continuing to support X.25. Recent development, however, has shown that X.25 can operate at T1/E1 (1.5/2.0 Mbps) speeds, which has helped the scalability of this solution.

Additionally, in today's telcos, many proprietary network management interfaces are being slowly phased out. One of the protocols that will remain in North America is Transaction Language One (TL1). It is a MAN (this should be changed to human or left as lower case "man" since it refers to a person and not a metro area net)-readable, text-based format for sending alarms to NMA (Telcordia Technologies' network monitoring and surveillance system) and other vendors' OS systems. TL1 is transportable as ASCII data either asynchronously via PAD services or over serial connections such as X.25, TCP/IP, and OSI. Other proprietary protocols consist of E2A, TBOP, TBOS, and several others that can be supported by several niche manufacturers.

Furthermore, while OS systems are adding support for IP interfaces, SONET/SDH equipment was designed using OSI/TP4. This has created a problem of incompatibility between systems. It also has driven a need in the area of protocol translation or mediation to enable the newer IP-based NMA applications to talk to legacy X.25 devices and to newer OSI based NE's. This incompatibility has caused confusion and complications within the DCN because the knowledge base among the support personnel of OSI is scarce worldwide. Many U.S. telco IT departments prefer to push OSI out to the far edges of the network so they only have to manage an IP backbone network and have the network support organization deal with the OSI issues in the central office NE. In Europe, GNE to OSS connectivity is OSI base. In the U.S., industry is beginning a movement toward IP to the SONET GNE (gateway network element). The GNE will in turn perform mediation to OSI on the SONET ring. However, not all vendors using OSI have made this committed move. Hence, OSI routing will remain in the DCN in many implementations.

Figure 2 Disparate networks and NOCs



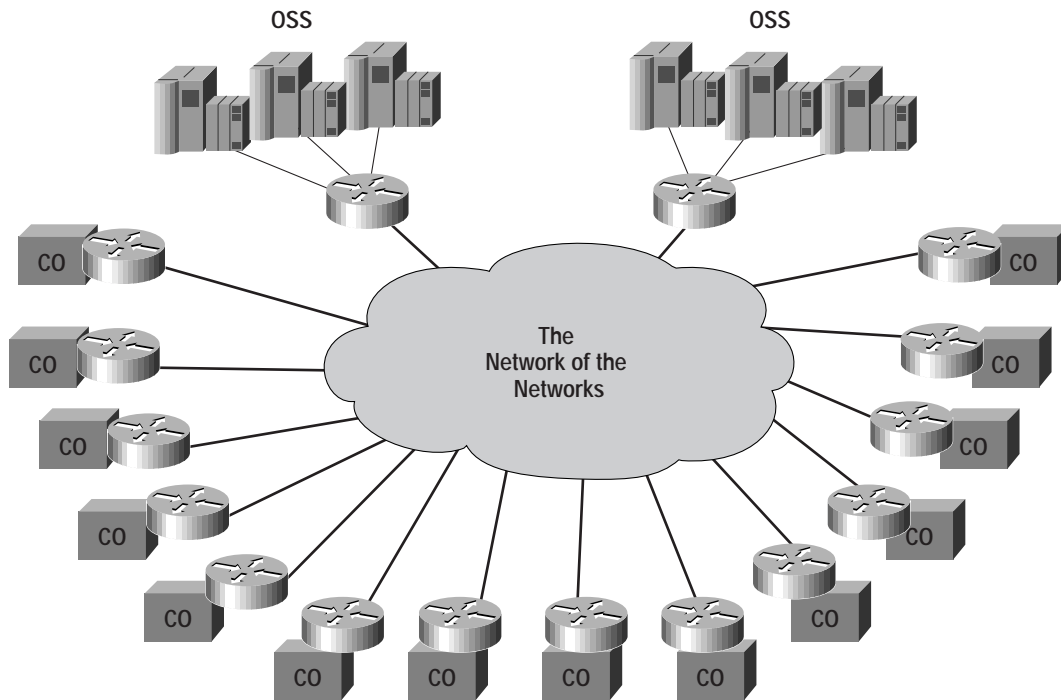
As a result of the above issues of incompatibility, past network implementers have been required to segregate the X.25 data onto a dedicated network, LAN-to-LAN traffic onto a new IP backbone and OSI traffic onto another network. In some cases, the IP backbone is also transporting the OSI traffic. At the end points, the implementers have had to glue on pieces of other hardware offered by niche vendors to provide proprietary protocol connectivity. The management of these various disparate DCN networks as depicted in Figure 2 is very challenging. Disparate networks add to the total cost of maintaining the different applications in the form of personnel, training, network operation center (NOC) platforms and their associated proprietary software applications.

The above are some of the hurdles that are driving the user community to implement end to end solutions from vendors who can support connectivity to existing telephony technology NEs as well as New World technologies.

The Need for a Better Solution

The "network of networks" is a vision of one autonomous infrastructure that can scale for growth on demand as well as serve all present and future networking requirements. One network that can connect the current telephony technologies as well as connect technology which enables the New World central office. This is the vision that enables telcos to realize tremendous technical benefit as well as substantial overhead cost reductions. The intent is to not change central office NEs but to offer a connectivity alternative for transport. Cisco has the expertise and product set to enable the telco's "network of networks" vision.

Figure 3 The Network of Networks



Technical DCN Implementation Details

DCN networks have existed for many years, and the mix of many different legacy network elements with newer technologies has necessitated different DCNs for connectivity to their OSS. Reasons for not transporting newer protocols over the existing infrastructure are scaling, network bandwidth restrictions as a result of the backbone protocol, philosophical decision to not put New World technology on top of the Old World network as well as many others. The following is a description of the various protocols and how they are being transported today.

Environments—Disparate Networks

2.1.1 X.25 Infrastructure

X.25 is a very mature technology that is still the work horse in many worldwide DCN infrastructures. Between the years of 1970 and 1987, X.25 was the de facto standard of data communications and was used extensively as the backbone technology of the many public and private data networks such as the Telco DCN. Every device and OSS in the network had some form of X.25 connectivity by either an X.25 serial interface or via X.25 Packet Assembler Disassembler (PAD) services for asynchronous connectivity. Since asynchronous ports on an NE can only support one user at a time, resource contention was an issue. As a result, a majority of the NEs had X.25 interfaces installed because X.25 is able to support many two-way virtual connections without having to be concerned with resource contention issues.

Today, X.25 is no longer the prevalent backbone technology of choice yet there are many years of investment in this infrastructure which requires that X.25 be supported in one form or another for quite sometime. Much of the older switching and transmission equipment is still managed by means of X.25 interfaces. These include products manufactured by Lucent, Nortel, Fujitsu, Tellabs, Ericsson and many others. In most cases, these interfaces can not be upgraded to IP since cost may be prohibitive or no upgrade migration path exists. Vendor development of X.25 products diminished as development resources were refocused onto Ethernet IP/OSI hardware interfaces. Today, the strategy of all telco network planners is to remove the X.25 backbone and transport the X.25 traffic over TCP via XOT over IP which is RFC 1613, discussed below.

BX.25 Connectivity

Many voice switch manufacturers use the BX.25 interface on the maintenance port. Introduced in the early 1980s by AT&T Bell Laboratories, BX.25 contains many of the features standardized in the 1984 ITU X.25 Standards and also some special features above Layer 3. BX.25 interfaces can be found on products such as the Lucent 5ESS/4ESS, Lucent 1A, Nortel DMS100 and Siemens EWSD. These voice switches are still in use today by many U.S. Regional Bell Operating Companies (RBOCs), IXCs, and CLECs.

A majority of the network backbones that transport BX.25 are X.25 based since they are compatible and share the backbone with other X.25 traffic. These implementations require customized protocol mediation at the BX.25-X.25 network interface. As IP backbone networks are deployed, all telcos are planning migration strategies to transport the BX.25 protocol over their IP backbone. It has been shown that BX.25 can be transported over IP as specified in RFC 1613. It only works when both the NE and OSS are BX.25.

TL1 Transport

Transaction Language 1 (TL1) is the most widely used management protocol in telecommunications. It is a man-machine, text-based message set (specified in Telcordia GR-833) that manages most of the broadband and access networks in North America and is increasingly being used worldwide for newer management applications. TL1 is also the preferred Command Line Interface (CLI) for telecom network elements. TL1 is the protocol for Telcordia's Network Monitoring and Analysis System (NMA) which is used for fault management of network elements. It is believed that TL1 will be used for management of network elements in COs for years to come. It can be transported via X.25, BX.25, TCP/IP and OSI.

Asynchronous Connectivity

The asynchronous devices have classically been connected to X.25 PADs for access to X.25 OSS applications. Most of these devices and interfaces will remain in the CO for some time to come but no new equipment is being deployed that have this interface.

IP Infrastructure

The "network of networks" will use IP as the backbone switching fabric for the future DCN. Today's OSS application hosts are being shipped with IP protocol stacks as the native interface although some have OSI/TP4 protocol stacks available as well. Remote intelligent applications are being installed in the central office that reside on workstations connected via Ethernet interfaces to a Local Area Network (LAN) communicate directly with the OSS using IP. Additionally, all of the newer central office devices are being shipped with IP interfaces except for most SONET/SDH network elements ship with OSI. Much work and planning is being invested in migrating all X.25, asynchronous, BX.25 and OSI/TP4 traffic onto the new IP infrastructure. By collapsing all of the DCNs to the "Network of Network", this will enable telcos to begin reducing network operating and support costs in the future.

OSI

From the SONET or SDH perspective, OSI has been the strategic direction of new network element platform manufacturers. However, there is industry movement to go to an IP interface on the GNE while OSI remains on the ring DCC. On the OSS application side however, we are finding more systems migrating towards IP. The resulting differences in protocols are creating a connectivity problem, OSI on the NE communicating with the IP OSS. OSSs such as NMA, and OSI NetExpert can have OSI interfaces as well as IP interfaces, and can be used in conjunction with implementing IP as the core backbone. Running OSI end to end is the best connectivity in the event that both the OSS and NE's have OSI interfaces. This would require tunneling the data end to end over TCP (IP backbone) or using OSI routing protocols if the backbone uses integrated ISIS or ISIS.

Cisco IOS Software

Cisco IOS software, which runs on more than 80 percent of Internet backbone routers, provides complete network services and enables networked applications for the DCN environment. Cisco IOS software provides the intelligence of the Internet through a suite of value-added technologies and features. It is the unifying thread that connects otherwise disparate hardware and provides security, reliability, and investment protection in the face of network growth, change, and new applications. It comprises a sophisticated suite of networking capabilities that reside at the heart of such internetworking devices as stand-alone routers, router modules for shared-media hubs, switches, PC and workstation file servers, and multi-service WAN access switches, Cisco IOS software differentiates Cisco internetworking solutions from other industry alternatives.

Cisco's Technical Solution

The Cisco IOS software, the industry-leading, standard-based IP implementation enables service providers to consolidate existing DCN environments into an integrated network of networks with the richest set of options available today.

The Cisco solution also can offer recommendations to some other current technological challenges. The major driver in this environment is the SONET/SDH hardware market expansion and the desire for all telcos to manage one common data communications network while retiring older legacy networking equipment in their DCNs. In all cases, Cisco has taken existing protocol implementations and enhanced them with out deviating from the intent of the mechanisms involved.

Cisco has created a specialized Cisco IOS product called the Cisco IOS Telco Feature Set. The Telco Feature Set is a tightly contained bundle of protocol support that is specific to the central office DCN. It encompasses all of the protocols that are specific to the CO such as IP routing, OSI/CLNS support as well as all of the various X.25 services. Below is a list followed by detailed descriptions of the various protocols and features contained in this package.

- IP Routing Services
- OSI/CLNS Support
 - Multiple OSI Area support per router
 - ISL for CLNS
- TL1 Support
 - Transport via X.25, TCP or OSI
 - TARP (TID Address Resolution Protocol)
 - TARP Storm Avoidance
- Bridging
- PPP Services
- WAN interface support for:
 - ISDN, Frame Relay, ATM, X.25
- X.25 Support Services
 - X.25 switching, X.3 Asynchronous PAD, DNS for X.25 address resolution, Hunt Groups, SVC/PVC conversion, Asynchronous Call Queuing
- IP to X.25 Protocol Translation
- BX.25 Transport over X.25 or TCP (XOT)

IP Services

In addition to IP and TCP, the Cisco TCP/IP implementation supports ARP, RARP, ICMP, Proxy ARP (in which the router acts as an ARP server on behalf of another device), Echo, Discard, and Probe (an address resolution protocol developed by Hewlett-Packard Company and used on IEEE 802.3 networks). Cisco routers also can be configured to use the Domain Name System (DNS) when host name-to-address mappings are needed.

BGP

BGP represents an attempt to address the most serious of EGP's problems. Like EGP, BGP is an interdomain routing protocol created for use in the Internet core routers. Unlike EGP, BGP was designed to prevent routing loops in arbitrary topologies and to allow policy-based route selection.

Access Restrictions

Most networks have reasonably straightforward access requirements. To address these issues, Cisco implements access lists, a scheme that prevents certain packets from entering or leaving particular networks.

A set of other access restrictions is provided by the Department of Defense-specified security extensions to IP. Cisco supports both the Basic and the Extended security options as described in RFC 1108 of the IP Security Option (IPSO). Support of both access lists and the IPSO makes Cisco a good choice for networks where security is an issue.



Tunneling

The Cisco TCP/IP implementation includes several schemes that allow foreign protocols to be tunneled through an IP network. Tunneling allows network administrators to extend the size of many networks beyond the size that their native protocols can handle.

Suppressing Network Information

In some cases, it may be useful to suppress information about certain networks. Cisco routers provide an extensive set of configuration options that allow an administrator to tailor the exchange of routing information within a particular routing protocol. Both incoming and outgoing information can be controlled using a set of commands designed for this purpose. For example, networks can be excluded from routing advertisements, routing updates can be prevented from reaching certain networks, and other similar actions can be taken.

Administrative Distance

In large networks, some routers and routing protocols are more reliable sources of routing information than others. Cisco IP routing software permits the reliability of information sources to be quantified by the network administrator with the administrative distance metric. When administrative distance is specified, the router can select between sources of routing information based on the reliability of the source. For example, if a router uses both IGRP and RIP, one might set the administrative distances to reflect greater confidence in the IGRP information. The router would then use IGRP information when available. If the source of IGRP information failed, the router automatically would use RIP information as a backup until the IGRP source became available again.

Routing Protocol Redistribution

Translation between two environments using different routing protocols requires that routes generated by one protocol be redistributed into the second routing protocol environment. Route redistribution gives a company the ability to run different routing protocols in workgroups or areas where each is particularly effective. By not restricting customers to using only a single routing protocol, Cisco route redistribution feature minimizes cost while maximizing technical advantage through diversity.

Cisco permits routing protocol redistribution between any of its supported routing protocols. Static route information can also be redistributed. Further, defaults can be assigned so that one routing protocol can use the same metric for all redistributed routes, thereby simplifying the routing redistribution mechanism.

Network Monitoring and Debugging

With today's complex, diverse network topologies, a router's ability to aid the monitoring and debugging process is critical. As the junction point for multiple segments, a router sees more of the complete network than most other devices. Many problems can be detected and/or solved using information that routinely passes through the router.

OSI Support

Cisco Systems was the first company to support dynamic interdomain routing within OSI environments. Currently, the Cisco OSI implementation provides both static and dynamic packet forwarding and routing and adheres to relevant ISO protocol specifications, including:

- ISO 8473 (CLNP)
- ISO 8348 (CLNS)
- ISO 8348/Ad2 (NSAP addressing)
- ISO 8208 (packet-level CONS)
- ISO 8802-2 (frame-level services on LAN media)
- ISO 8881 (CMNS over ISO 8802-2)
- ISO 7776 (Link Access Procedure, Balanced)
- ISO 9542 (ES-IS)
- ISO 10589 (IS-IS)

Integrated IS-IS extensions for IP as defined in RFC 1195 also are supported. Users can perform CLNP routing over Ethernet, Fiber Distributed Data Interface (FDDI), Token Ring, and serial line networks. The Cisco OSI implementation is also compliant with the United States Government Open Systems Interconnection Profile (US-GOSIP) Version 2 specification, and Cisco is the first router vendor to be certified and registered with the National Institute of Standards and Technology (NIST).

Interoperability

The ability of protocol implementations to work with other implementations of the same protocol (often called interoperability) is a critical feature of any OSI implementation. The Cisco OSI implementation is highly interoperable, having been proven so in OSI interoperability demonstrations with AT&T, Data General, DEC, Frontier Technologies, HP, IBM, Intel, NCR, Novell, OSiWare, Spider, Sun, Tandem, Touch, Unisys, and Wollongong. Cisco routers are able to interoperate with equipment from each of these vendors, a fact that is particularly noteworthy in the case of AT&T, which many people believe has the largest installed base of CLNP end systems. Cisco also participated successfully in a European pilot demonstration of CLNP-protocol-based inter-domain routing.

Route Redistribution

Cisco routers support information sharing between multiple routing protocols and between multiple instances of the same routing protocol. Such sharing is known as route redistribution and is supported among all Cisco routing protocols. Route redistribution ensures that routing can occur in networks that run multiple routing protocols. This is achieved by creating route maps. Route maps give network managers unprecedented control over the ways that routing information is propagated in their networks. Redistribution configuration files that use route maps are easy to create, understand, and modify. Using route maps, Cisco users are able to build larger, more robust, reliable networks, with better traffic control than ever before.

OSI Filtering

Cisco offers advanced filtering features that provide additional administrative control of traffic flow in an OSI network. There are four components to a Cisco OSI filter:

1. Address templates are applied to NSAP addresses to provide flexible filtering based on all or a portion of the address.
2. Also, address templates can be assigned names called template aliases for ease of use.
3. A filter set is a named collection of address templates with associated permit/deny indications.
4. Cisco offers other filter expressions, and certain logical operators (AND, OR, XOR, and NOT). Filter expressions allow filtering combinations not possible with simple filter sets. Further, they permit matches on source address. Filter sets and filter expressions can be applied to inbound or outbound CLNP datagrams, IS-IS adjacencies (IS-IS routers that are on the same network segment), ISO-IGRP adjacencies, ES-IS adjacencies, and route redistribution to save time and avoid configuration errors.

Integrated and Interdomain Routing

In addition to Cisco support of Integrated IS-IS, its standard IS-IS implementation still can run simultaneously in the same router with other routing protocols. In addition to Integrated IS-IS, Cisco continues to offer its ISO-IGRP implementation.

Other Features

To provide monitoring and troubleshooting capability, the Cisco CLNP implementation supports both ping and trace commands. Ping and trace commands translate into less time spent debugging network problems.

X.25 Switching

Cisco support of ISO 8208 (CONS) provides the ability to extend X.25 switching to different media, such as Ethernet, Token Ring, and FDDI. CMNS specifies the implementation of packet-level X.25 over the Logical Link Control 2 (LLC2) connection-oriented data link service on LAN media. LAN-based OSI nodes can be connected both to one another and to remote OSI-based DTE devices via X.25 public data networks (PDNs) or point-to-point lines. The name CMNS has been changed and is now known as Connection-Mode Network Service (CMNS).



Multiple OSI/IS-IS area support per router

Multiple OSI/IS-IS area support addresses the problem directly by allowing multiple level-1 areas to be supported in a single router. From a user perspective, multiple ISIS instances may be defined, each with a separate area address. Individual interfaces are then assigned to different instances (level-1 areas). A single Level 2 area continues to exist to provide access to the backbone. The router also provides connectivity between level-1 areas local to the router.

This feature replaces several routers with one and saves central office space.

Restrictions

Cisco IOS software is capable of supporting up to 12 instances (OSI Areas) in a single Cisco 3662-DC-CO router. Other considerations (resource constraints, especially CPU) may further limit the number of areas that may be supported in practice. Three instances can be supported in a Cisco 2600 Series router.

Manual Area Addresses

Manual Area Addresses (MAA) enable OSI areas to be combined without having to readdress, such as if you configure multiple area addresses on a router, ISIS merges those areas into a single area. Cisco has increased support for Manual Area Addresses from 3 to 256 MAAs.

TL1 Transport

With Cisco's Protocol Translation service, TL1 can be transported via X.25, BX.25, OSI/TP4 and TCP/IP as payload data.

TL1 to NSAP address resolution (TARP)

TL1 identifies network elements by means of a target identifier (TID) which have no correlation to the devices' network addresses. This makes it necessary for a particular device to cache the address mapping between a TID, and its corresponding network address. Since these applications run mostly over OSI, the network addresses involved are OSI NSAPs. When an NE sends a packet to another NE or OSS, it does not have information about the NSAP corresponding to the remote device's TID. A mechanism to request this information from an intermediate router along the network is now supported by Cisco as an address resolution protocol called Target Identifier Address Resolution Protocol, or TARP.

TARP Storm Avoidance

The NE's use TARP to identify themselves to the OSS. A problem exists when a small number of NE's go into a reset condition which in some cases would force the NE to fail. The resulting Type 4 TARP traffic is so high that other NE's begin resetting themselves and the entire cloud cascades down into a TARP storm with all of the broadcasting messages proliferating through out the network. To avoid TARP storms, Cisco has implemented a mechanism that selectively sends only certain type of messages and suppresses others.

RFC 1613—XOT.

RFC 1613 is a Cisco initiative that is known as XOT. XOT allows for the transport of X.25 packets over a TCP backbone infrastructure and is insensitive to the DTE/DCE role of the local interfaces at either end of an XOT TCP connection. Transport can originate from an X.25 DTE device or can be PAD originated traffic and allows the router to transport X.25 VCs transparently over a TCP connection on a one-to-one basis; one VC creates one TCP connection. This implementation is symmetrical and requires that another RFC 1613-compliant device such as a Cisco router be on the other side of the network to strip the TCP and IP header information for delivery to the remote X.25 device. XOT can transport the Bellcore standard known as BX.25.

X.25 Support

Cisco believes that X.25 will be in the telco DCN beyond the year 2000 and we are committed to supporting this protocol through its natural migratory path. Cisco has rewritten the X.25 engine, XPE, by making it more modular. The enhancement takes advantage of common internal pathways as well as new Cisco IOS operating system enhancements to make the implementation very robust. Cisco's goal is to allow Cisco IOS technologies to coexist in any enterprise network infrastructure. Cisco's X.25 enhancement goal is to continue to:

- Adhere to the X.25 International Telecommunications Union Telecommunication (ITU-T) standards previously known as the International Telegraph and Telephone Consultative Committee (CCITT)
- Develop features that have specific requirements that are a global requirement such as SVC to PVC conversion.
- Provide packet-switching capabilities with innovative value-added network services such as DNS routing for X.25 and protocol translation.

Async PAD support

The Cisco X.28 packet assembler/disassembler (PAD) supports all X.3 parameters, all X.28 and X.29 ITU-T 1988 standard commands. They allow a user to review, modify X.3 parameters and place calls. Cisco has implemented several extended X.28 commands that enhance the functionality of the PAD. PAD operation (both standard and protocol translation) can be configured to use X.25 or XOT directly. Cisco PAD services also support the use of mnemonics, reselect, bidirectional PAD, async port sub addressing and many other crucial features.

X.25 to IP Protocol translation

Protocol translation (PT) software allows bidirectional translation between Digital Equipment Corporation (DEC) local-area transport (LAT), X.25, and TCP environments. The Serial Link Protocol (SLIP), Point-to-Point Protocol (PPP), and Appletalk Remote Access Protocol (ARAP) are async protocol modes supported by the PT as an inbound "Virtual Async" (vty async) connections only. Virtual async connections allow the user to access a common environment through async devices that don't support async protocols. Vty async provides the ability to tunnel a remote node network protocol such as IP or IPX over PPP, across a network backbone that does not have native support of the protocol. Protocol translation uses PAD services, but PAD is not dependent on protocol translation services to function. Protocol translation is a nonspecific WAN implementation that allows transport over a Frame Relay, IP, or X.25 backbone.

DNS routing for X.25

This is a Cisco only feature, which addresses one of the major problems that the network administrator faces in maintaining an X.25 access network over an IP backbone. This feature uses a centralized DNS database for X.121 to IP address query and resolution.

BX.25 transport

Cisco has validated that BX.25 can be transported directly over X.25 or over an IP infrastructure using RFC 1613. To transport BX.25, you must disable the Unnumbered I-Frames being sent from the NE to the Cisco router. I-Frames are used to carry a password between the host and the telephone switch, which is very similar to an XID.

Software Release Information

As mentioned, Cisco has created the Cisco IOS Telco Feature Set, which is a tightly contained bundle of protocol support that is specific to the central office DCN. The newly created feature set is available in Cisco IOS Version 12.0(5)T and higher, and was released in June of 1999.



Cisco Platform Product Support

Cisco IOS software is available on all Cisco router products in various protocol application packages called images. IP and X.25 services are base products available in the IP image. Support for both OSI and Protocol Translation are available in the Cisco IOS Telco Plus Feature Set (enterprise image for most platforms). The feature set is a specialized telco image available only on the new 3660 platform. This tightly defined Cisco IOS package supports IP, X.25/PAD, IP/X.25 Protocol Translation, and all OSI services.

3660 Platform Description

The new 3660 platform was designed and built with the telco central office as its initial primary mission. It is a high performance six-slot, NEBs/ETSI-compliant platform from the 3600 product line. Basic characteristics of this new platform that became available in June of 1999 are as follows:

- 5 FRU chassis
- 6 network module slots (NMs)
- Performance: 120-Kpps Fast Switch, 12-15K process switch
- 2 Internal Advanced Interface Module (AIM)
- Slots: for compression/encryption, and so on
- 2 FE 10/100-Mb integrated on motherboard, w/ ISL, TX only
- 2 PCMCIA slots, console, aux
- CO/ NEBs-Ccompliant: 12-inch deep, including cable drape
- Center mounting brackets
- Dual DC power
- Redundant hot-swap power supply
- Hot swap of like network modules using OIR (Online Insertion and Removal)
- Cable guides
- CLEI coding
- Telco software SKU with the new Cisco IOS Telco Feature Set loaded Cisco IOS Telco Plus Feature Set available as an optional upgrade

Cisco Contacts

This section will detail the product management contacts

Pepe Garcia—product manager for the routing protocols

Murali Kolli—product manager for X.25 and protocol translation

Sarat Khilnani—product manager MPSBU

Wayne Yamaguchi—product manager, Service Provider Marketing



Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
<http://www-europe.cisco.com>
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

Americas
Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-7660
Fax: 408 527-0883

Asia Headquarters
Nihon Cisco Systems K.K.
Fuji Building, 9th Floor
3-2-3 Marunouchi
Chiyoda-ku, Tokyo 100
Japan
<http://www.cisco.com>
Tel: 81 3 5219 6250
Fax: 81 3 5219 6001

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the
Cisco Connection Online Web site at <http://www.cisco.com/go/offices>.

Argentina • Australia • Austria • Belgium • Brazil • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela