

Wired network architectures encountered at customer sites fall into two classifications: switched Layer 2 networks or routed Layer 3 networks. The fundamental difference between these network types is the communications protocol layer relied upon for propagating data across network resources. An understanding of layered communications protocols and the underlying services extended by the individual layers is necessary to understand these differences.

UNDERSTANDING THE OSI NETWORK REFERENCE MODEL

The International Standards Organization (ISO) publishes a reference prototype for networking protocols, referred to as the Open Source Interconnect (OSI) model. The OSI model abstracts information transfer requirements into distinct services, and organizes these services into seven functional layers. Table 1 briefly describes these layers, their associated services, and protocols supported.

The upper layers—layers 4 through 7—deal with application issues and are generally only implemented in software. The lower layers—layers 1 through 3—handle data transport issues. The physical layer and the data link layer are implemented in hardware and software. The amalgamation of these functional layers is referred to as a network stack.

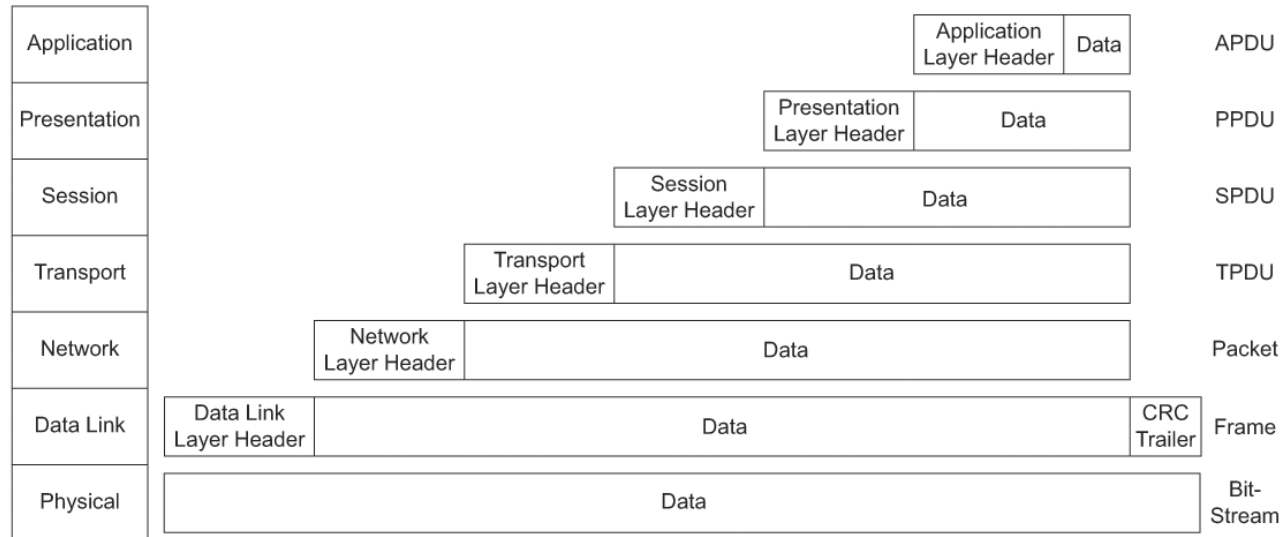
Table 1 — OSI Model Layers

Layer	Function	Service Description	Examples
7	Application	The Application layer represents the interface at which applications access network services. This layer represents the services that directly support applications such as software for file transfers, database access, and electronic mail.	FTP; Telnet; NFS; HTTP
6	Presentation	The Presentation layer translates data from the Application layer into an intermediary format. This layer also provides services such as data encryption, and data compression.	ASCII; HTML; JPEG
5	Session	The Session layer allows two applications on different computers to establish, use, and end a session.	SQL; RPC
4	Transport	The Transport layer defines the end-to-end transmission of data between nodes, including flow control and error recognition and recovery. It also repackages long messages when necessary into smaller packets for transmission and, at the receiving end, rebuilds packets into the original message.	TCP; UDP; SPX
3	Network	The Network layer provides logical network addressing, path determination, media/framing translation, frame fragmentation, and congestion signaling/control.	IP; X.25; IPX; Q.931
2	Data Link	The Data Link layer packages raw bits from the Physical layer into frames (logical, structured packets). This layer specifies the device addressing, topology and media access, bit/byte synchronization, flow control, and error detection/recovery services associated with sending frames of data over a physical link.	HDLC; Ethernet; LLC; Frame Relay; ATM; Q.921; FDDI
1	Physical	The Physical layer specifies how bit streams are to be transmitted over a physical link in the network. Includes mechanical, electrical and procedural characteristics of device interconnection	RS-232; V.35; 10bT; RJ48C G.703/G.704

Within the network, information traverses a network stack using a process called encapsulation. When an application requires communications resources, the message is handed over to the network stack's application layer. There, the message is processed into a Protocol Data Unit (PDU).

Each subsequent layer in the source system's network stack adds service-specific header information to the PDU, until a fully formatted data frame is presented to the physical layer for transmission onto the communications medium. This encapsulation process is illustrated in Figure 1.

Application specific header information is prepended to (or wrapped around) the data. The resultant PDU is then passed to the stack's presentation layer, where additional header information is added.

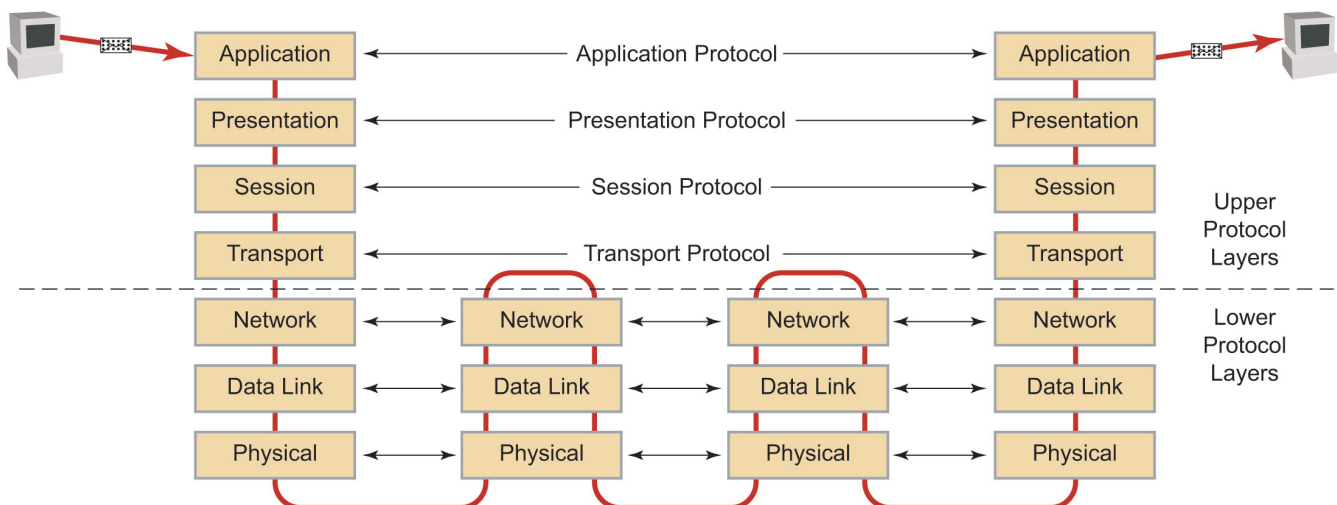


NF0001

Figure 1 — Encapsulation Process

When the bit stream reaches the destination system, the reverse occurs. Each layer in the destination system's network stack analyzes and then strips its associated header information from the message. The resultant PDU is then passed to the next higher layer, until the original message is presented to the destination application.

Typically, a communication layer does not process, or alter the PDU's content as generated by an adjacent layer. Information exchange only occurs between peer OSI layers. The peer relationship between OSI layers is illustrated in Figure 2.



NF0002

Figure 2 — Peer Relationship between OSI Layers

SWITCHING OVERVIEW

The predominant LAN technology deployed in the marketplace today is derived from the original Ethernet specifications. Ethernet is a shared media LAN technology that leverages Carrier Sense Multiple Access with Collision Detection (CSMA/CD) for media access procedures. These rules dictate that an Ethernet station monitor the cable medium for absence of signal carrier as a prerequisite to sending data.

For those occurrences when multiple stations simultaneously transmit, the collision detection component of the protocol forces those stations to cease transmission, and retry after a randomly generated delay period. This non-deterministic media access control is a low-cost, easily scaled solution for interconnecting networked stations.

However, as media utilization increases from higher traffic demands and from the attachment of additional stations, the cumulative channel idle time diminishes. As a result, overall network performance will degrade as contending stations wait for channel access. This condition is further exasperated by the increased collision rates as networked stations compete for diminishing channel bandwidth.

Ethernet switches provide a solution for the performance degradation problems associated with media saturation. An Ethernet switch is an intelligent Layer 2 networking appliance that can restore near wire-speed bandwidth to attached devices.

By allocating an access port for each station, cable bandwidth is dedicated to the attached device. Internally, the switch associates its attached station's Ethernet address information, known as the MAC address, to physical port ID's within a cache table.

As ingress traffic arrives on a switch port, the frame's destination address is assessed by the switch's logic, and if a cache entry exists, the frame is forwarded to the switch port servicing the destination device.

By insulating unicast traffic (data transmissions between explicit end-points) from non-involved stations, simultaneous transmissions on the LAN are now possible. This being the case, a switched-Ethernet network provides two immediate benefits over a shared-media Ethernet design:

- A device's dedicated use of the interconnecting medium (to the switch) eliminates the contention for wire access
- The theoretical bandwidth of the LAN is now the aggregate sum of the wire-speeds of the switch's ports, or the switch's internal bus bandwidth—whichever is less

Collision vs. Broadcast Domains

A shared-media Ethernet network is also referred to as a "collision domain". Seemingly redundant when applied to a shared cable (for example, obsolete 10b5/10b2 coaxial cable-based bus topologies), this also applies to Ethernet hub-based designs, where a passive hub device interconnects dedicated wire runs to the LAN stations.

Collision domains exist where the CSMA/CD rules are required to arbitrate media access. When using an Ethernet switch, each port establishes a new collision domain.

When servicing a single network station, the need for CSMA/CD to manage contention is irrelevant except if a downstream hub device is used to connect multiple stations to the switch. Within a collision domain, all stations have visibility of all traffic generated by the other stations.

In addition to unicast traffic, LAN stations generate broadcast traffic, or messages implicitly directed to all other stations on the LAN. Broadcast messages are propagated through all switch ports, to all stations within a logical network.

The boundary within which messages are propagated is referred to as a "broadcast domain". In most circumstances, broadcast messages are considered necessary overhead traffic, allowing device configuration, status reporting, event signaling, etc. Examples of these types of traffic include (but are not limited to):

- BootP/Dynamic Host Configuration Protocol (DHCP) server requests
- Address Resolution Protocol (ARP) queries
- Service (e.g., file-sharing, printer, etc.) announcements
- Spanning Tree Protocol (STP) exchanges
- Routing protocol exchanges/updates

The relationship of collision domains and broadcast domains is illustrated in Figure 3. Each collision domain includes an Ethernet switch port in addition to the indicated devices.

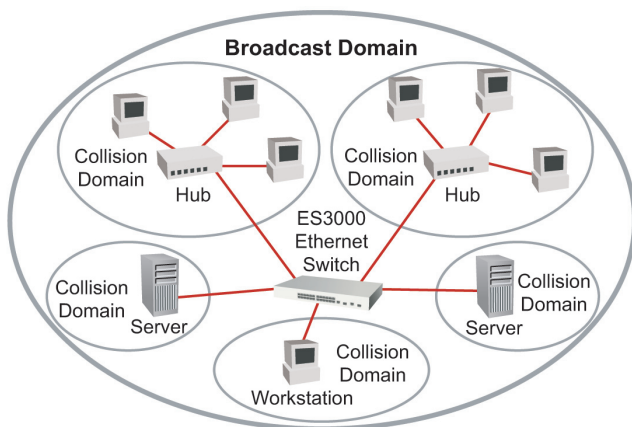


Figure 3 — Collision Domains vs. Broadcast Domains

NF0003

Network Expansion Pitfalls

Multiple Ethernet switches may be interconnected as a means to expand the number of devices within a broadcast domain. By using Ethernet bridges, a broadcast domain may be further extended via Wide Area Network (WAN) facilities.

As a switched network is expanded, it becomes desirable to introduce redundant links, or alternate path connections with the intent to minimize the impact of network faults. However, this design also ends up introducing communication loops.

A communication loop presents a problem for a Layer 2 switched network because broadcast traffic is perpetually forwarded until it saturates the bandwidth capacity of the network, consequently starving resources from all other stations. This can lead to a fault referred to as a “broadcast storm” where all network bandwidth is consumed by broadcast messages. A broadcast storm can very quickly render a network useless.

Spanning Tree Protocol to Prevent Network Loops

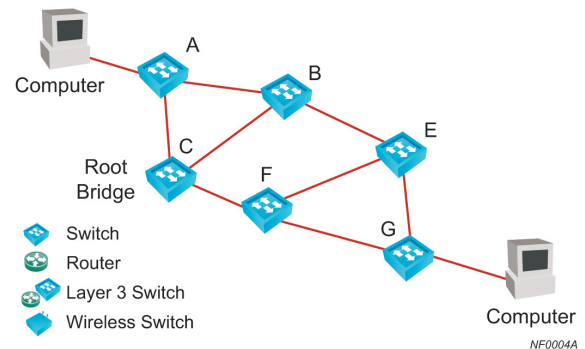
To counter broadcast storms, Ethernet switches and bridges implement the IEEE 802.1d Spanning Tree Protocol (STP) to prevent network loops.

An STP network elects a root node, which then advertises its status by broadcasting Bridge Protocol Data Unit (BPDU) messages. Network appliances or nodes within the broadcast domain listen for BPDU messages, noting from which ports the messages arrive.

When downstream nodes receive BPDUs via multiple ports, they determine which port is ‘closest’ to the root bridge, and then block the other BPDU-receiving port(s) from forwarding frames (thus disabling a source of a network loop). When all STP nodes in a broadcast domain complete this topology-learning process, the network is considered converged and loop-free.

The remaining unblocked ports transition to a forwarding state and normal frame-forwarding operations are resumed. Should a network fault disrupt communications, an event notification gets forwarded to the root bridge, and this convergence process is repeated until a new loop-free topology has been learned.

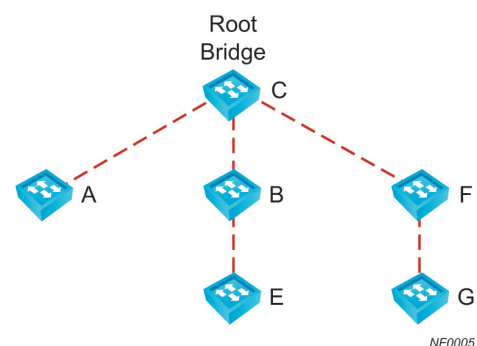
Figure 4 illustrates the effect of an STP operation; six switches are interconnected in a meshed topology. While this topology offers the benefit of alternate paths in case any link interconnecting the switches fails, it also introduces multiple loops. STP BPDUs are propagated between the network switches to discover a loop free topology.



NF0004A

Figure 4 — Sample Switched Network Topology

Figure 5 presents a logical representation of this converged network map.



NF0005

Figure 5 — Logical View of Loop-free STP Network

As a result of STP convergence, the associated switch ports for links between switches A and B, E and F, and E and G are placed into blocking mode, and thus prevented from forwarding frames. The resulting operational topology is depicted in Figure 6:

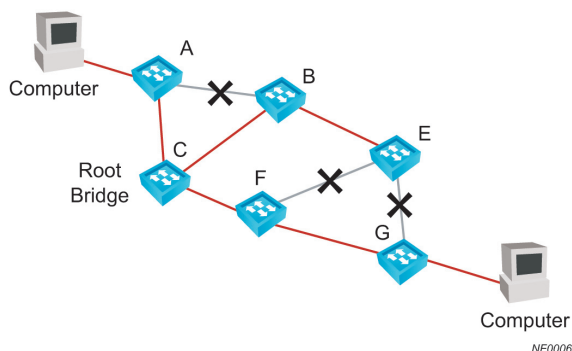


Figure 6 — Converged STP Network Topology

VLAN SEGMENTATION

As LANs expand to service larger numbers of users and applications with disparate networking requirements, it becomes beneficial to split the LAN into separate broadcast domains. Advanced LAN switches have the ability to allocate switch ports into closed user groups referred to as Virtual LANs (VLANs).

Each VLAN establishes an independent broadcast domain, and restricts frame flows to ports assigned to common a VLAN (or closed user group participants). A VLAN may be extended between multiple LAN switches.

To expand VLANs across multiple switches, a link dedicated for each VLAN is necessary. Reasons to consider LAN segmentation include:

- Reducing the detrimental impact of excessive broadcast traffic on LAN performance
- Insulation of application traffic (that is, separating voice traffic from data traffic)
- Introducing inter-department security (that is, configuring LAN resources to restrict visibility and access of resources dedicated for a defined user group from users outside of the designated group).

Figure 7 illustrates VLANs bridged across two switches. This method implements two physical bridge links between devices, each link carrying the traffic for a specific VLAN.



Figure 7 — Bridging VLANs

VLAN TRUNKING

A more efficient approach to bridging multiple VLAN links between switches is to consolidate them into a single inter-switch bridge link. A VLAN trunk consolidates the traffic of multiple VLANs across a single physical port, while maintaining the benefit of inter-VLAN traffic isolation, as shown in Figure 8.



Figure 8 — VLAN Trunking

802.1q Standard for Bridged VLANs

One approach for carrying multiple VLANs on a single wire is using the IEEE 802.1q Standard for Virtual Bridged Local Area Networks. The 802.1q protocol is an internal tagging mechanism that inserts a 4-byte tag header within the existing Ethernet frame. This tag header is constructed of two fields:

- A two-byte tag protocol identifier (TPID) that contains a fixed value "0x8100." This tag denotes that the frame is carrying 802.1q tag information
- A two-byte tag control information (TCI) that carries the unique VLAN ID information

Alternative Proprietary Frame Encapsulation

Alternatives to 802.1q-compliant frame tagging are proprietary methods involving frame encapsulation. One such technique is Cisco System's Inter-Switch Link (ISL) protocol.

The ISL pre-standard technology wraps the unmodified Ethernet frame with 30-bytes of additional information, as follows:

- A 26-byte header field. Imbedded within this header is a 10-bit VLAN ID
- A 4-byte cyclical redundancy check (CRC) trailer field. This error check is in addition to the frame checking performed by the standard Ethernet frame processing

As traffic is directed across a VLAN trunk, it is first associated to its originating VLAN using the 802.1q standard tagging (or proprietary ISL encapsulation) mechanism. On the receiving end of the trunk, the tagging information is stripped and analyzed, with the standard formatted Ethernet frame forwarded to the destination port, or forwarded to the appropriate VLAN ports.

ROUTING OVERVIEW

Routing is the process of forwarding packets between LANs based on the logical addressing component found at Layer 3 of the protocol stack. Originally performed as resident software within mainframe and minicomputer platforms, modern routers have evolved into extremely high performance and feature rich networking engines. A basic router performs two principal functions:

- The router maintains a forwarding table, also called a routing table, constructed by static, administratively inserted routes, and/or by dynamically exchanging route information with its peers. The latter is accomplished using one, or an array of routing protocols
- The router uses the resultant forwarding table to direct ingress packets to the correct egress interface based on their logical Layer 3 network address information

Advantages of Routers vs. Switches

Routers provide several distinct advantages over switches in network implementations:

- Routers do not forward broadcast frames by default (though broadcast frames can be explicitly directed to a specific network). This allows VLANs to be designed for optimal performance (that is, smaller sub-networks that reduce the broadcast/total traffic ratios), using routing services to communicate between VLANs
- Since broadcast frames are not automatically forwarded, communication loops and their resultant broadcast storms are no longer a design issue
- Since communication loops do not represent a design flaw, redundant media and fully/partially-meshed topologies can offer traffic load sharing and more robust fault tolerance

FURTHER READING

Wireless Knowledge Center: www.symbol.com/products/wireless/Knowledge_Center.html

What is a Wireless Switch?: [ftp://symstore.longisland.com/Symstore/pdf/wireless/WirelessSwitchWP.pdf](http://symstore.longisland.com/Symstore/pdf/wireless/WirelessSwitchWP.pdf)

WS5100 Product Page: www.symbol.com/products/wireless/ws5100.html

WS2000 Product Page: www.symbol.com/products/wireless/ws2000_brochure.html

About Symbol Technologies

Symbol Technologies, Inc., The Enterprise Mobility Company™, is a recognized worldwide leader in enterprise mobility, delivering products and solutions that capture, move and manage information in real time to and from the point of business activity. Symbol enterprise mobility solutions integrate advanced data capture products, radio frequency identification technology, mobile computing platforms, wireless infrastructure, mobility software and world-class services programs under the Symbol Enterprise Mobility Services brand. Symbol enterprise mobility products and solutions are proven to increase workforce productivity, reduce operating costs, drive operational efficiencies and realize competitive advantages for the world's leading companies. More information is available at www.symbol.com.

Corporate Headquarters Symbol Technologies, Inc.

One Symbol Plaza
Holtville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

For Asia Pacific Area Symbol Technologies Asia, Inc.

(Singapore Branch)
Asia Pacific Division
230 Victoria Street #05-07/09
Bugis Junction Office Tower
Singapore 188024
TEL: +65.6796.9600
FAX: +65.6337.6488

For Europe, Middle East and Africa Symbol Technologies

EMEA Division
Symbol Place, Winnersh Triangle
Berkshire, England RG41 5TP
TEL: +44.118.9457000
FAX: +44.118.9457500

For North America, Latin America and Canada

Symbol Technologies
The Americas
One Symbol Plaza
Holtville, NY 11742-1300
TEL: +1.800.722.6234/+1.631.738.2400
FAX: +1.631.738.5990

Symbol Website

For a complete list of Symbol subsidiaries and business partners worldwide contact us at:
www.symbol.com
Or contact our pre-sales team at:
www.symbol.com/sales

Routing Protocols

A routing protocol is a combination of the learning algorithm that discovers the network topology, and the messaging format that facilitates information exchange between peered routing devices. The function of a routing protocol is to dynamically build and maintain routing tables that are used for path selection between routers.

Routed protocols contain a Layer 3 logical network component that is referenced to transport data packets through an inter-network to its ultimate destination. A routing protocol may be specific to the routed protocol it is designed to support. For example, NLSP will manage routing tables for IPX traffic, and AURP will manage routing tables for AppleTalk traffic.

Examples of routing protocols include:

- Routing Information Protocol (RIP), versions 1 and 2
- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Novell's Link State Protocol (NLSP)
- Apple's AppleTalk Update Routing Protocol (AURP)
- Cisco's Interior Gateway Routing Protocol (IGRP)
- Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)

symbol
The Enterprise Mobility Company™



TB NETFUND 04/05

Part No. TB NETFUND Printed in USA 04/05 © Copyright 2005 Symbol Technologies, Inc. All rights reserved. Symbol is an ISO 9001 and ISO 9002 UKAS, RVC, and RAB Registered company, as scope definitions apply. Specifications are subject to change without notice. Symbol® is a registered trademark, and The Enterprise Mobility Company is a trademark of Symbol Technologies, Inc. All other trademarks and service marks are proprietary to their respective owners. For system, product or services availability and specific information within your country, please contact your local Symbol Technologies office or Business Partner.