Glossary

December 2015

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Preface

This document defines terms used in IP Infusion's networking software products.

Conventions

This document uses the conventions described below.

Sort Order

The terms are arranged in ASCII order with the case of the characters ignored. This is the same as if the terms were sorted by this Linux command:

sort -f

This means that spaces, symbols, and digits come before alphabetic characters. Digits are sorted as strings, not numeric values ("10" comes before "2").

The exact ASCII collating sequence is as shown below, with a space character in the first position:

```
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
```

There are some exceptions to this rule when it makes more sense than strict ASCII order:

- (S,G) is under S
- G.8031 and G.8031 are under Numbers

Acronyms

The full phrase is shown before the acronym. For example:

- network address translation (NAT)
- Local Area Network (LAN)

An exception is when the acronym is used exclusively to refer to the term, in which case the acronym is shown before the full form:

- I-SID (Service Instance Identifier)
- NETCONF (Network Configuration Protocol)

When an acronym is part of a phrase and is defined separately, its full form is not shown:

- BGP confederation
- FEC-to-NHLFE (FTN) map
- GARP VLAN Registration Protocol (GVRP)
- MAC address

Case

As shown in the examples above, all lowercase is used for terms except when the predominant usage is initial uppercase or all uppercase.

Terms

Numbers

1588v2. IEEE specification for Precision Time Protocol (PTP).

802. A family of IEEE Local Area Network (LAN) standards. The services and protocols specified by the 802 standards map to Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model:

- 802.1: Overview architecture of LANs and interneworking
- 802.2: The logical link control (LLC) sublayer of Layer 2 (L2)
- 802.3: Layer 1 (L1) and the Media Access Control (MAC) sublayer of Layer 2 (L2), Also called Ethernet.

802.1AB. IEEE specification for Link Layer Discovery Protocol (LLDP).

802.1ad. Amendment to IEEE 802.1Q for Provider Bridging (PB).

802.1ag. Amendment to IEEE 802.1Q for Connectivity Fault Management (CFM).

802.1ah. IEEE specification that adds Provider Backbone Bridging (PBB) to 802.1ad Provider Bridging (PB):

802.1ak. Amendment to IEEE 802.1Q for Multiple Registration Protocol (MRP).

802.1aq. Amendment to IEEE 802.1D for Shortest Path Bridging (SPB).

802.1AX. IEEE specification for link aggregation and Multi-Chassis Link Aggregation (MC-LAG).

802.1D. IEEE specification which allows multiple LANs to be connected together through what the standard calls a “MAC bridge” which filters data sent between LAN segments, allowing networks to be partitioned for administrative purposes and reducing network congestion. The more common term for a MAC bridge is switch. The 802.1D standard includes Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP).

802.1p. IEEE 802.1Q defines priority signaling for traffic that can be used by Quality of Service (QoS) mechanisms to differentiate traffic. Packets are tagged as belonging to a queue, which determines the priority of the packet. Although this technique is often called “802.1p”, there is no standard by that name. Instead, the technique is incorporated into 802.1Q standard.

802.1Q. IEEE Virtual Local Area Network (VLAN) and Multiple Spanning Tree Protocol (MSTP) specifications. This standard refers to VLANs as “virtual bridged networks”. The 802.1D standard covers “VLAN-unaware” switches, while 802.1Q extends 802.1D for “VLAN-aware” switches.

802.1Qau. Amendment to IEEE 802.1Q for Quantized Congestion Notification (QCN).

802.1Qay. Amendment to IEEE 802.1Q for Provider Backbone Bridge-Traffic Engineering (PBB-TE).

802.1Qaz. Amendment to IEEE 802.1Q for Data Center Bridging Capability Exchange (DCBX) and Enhanced Transmission Selection (ETS).

802.1Qbb. Amendment to IEEE 802.1Q for Priority-based Flow Control (PFC).

802.1Qbg. Amendment to IEEE 802.1Q for Edge Virtual Bridging (EVB).

802.1v. Amendment to IEEE 802.1Q to classify incoming packets based on data link layer protocol identification.

802.1X. IEEE specification for port authentication.

802.3ah. IEEE specification for Ethernet to the First Mile (EFM).

802.3x. IEEE specification for flow control.

G.8031. ITU-T specification for Ethernet Linear Protection Switching (ELPS).

G.8032. ITU-T specification for Ethernet Ring Protection Switching (ERPS).

A

Access Control List (ACL). A set of rules used to filter traffic. Each rule specifies a set of conditions (such as source address, destination address, type of packet, or combination of these items) that a packet must meet to match the rule. When a device determines that an ACL applies to a packet, it tests the packet against the conditions of all rules. The first match determines whether the packet is permitted or denied.

access layer. In the network design model, the layer that connects devices such as desktops, laptops, servers, and printers to the network and provides end users access to network resources. This layer accepts traffic into a network and can pass that traffic to the distribution layer. The access layer is usually built using Layer 2 (L2) switching such as Spanning Tree Protocol (STP). This layer connects logical broadcast domains and provides isolation to groups of users. Typically, Virtual Local Area Network (VLAN) instances are implemented as broadcast domains in the access layer. Also called the edge layer. See also customer edge (CE), provider edge (PE).

acknowledgment (ACK). Notification sent from one network device to another to acknowledge that some event (for example, receipt of a message) has occurred.

active route. Route chosen from all routes in a Routing Information Base (RIB) to reach a destination. Active routes are installed in the Forwarding Information Base (FIB).

address. A unique identifier for a device on a network, either as a sender or receiver. An address can be a physical address or a logical address.

See also address family, address resolution, Classless Interdomain Routing (CIDR), domain name, Domain Name Service (DNS), dynamic address, IP address, MAC address, name resolution, static address.

address family. A specific type of network addressing supported by a routing protocol. Examples are IPv4 unicast and IPv4 multicast. See also subsequent address family identifier (SAFI).

address resolution. The process of translating the address of an entity on one system to the equivalent address of the same entity on another system. For instance, translating an IP address to its Domain Name Service (DNS) name. See also Address Resolution Protocol (ARP).

Address Resolution Protocol (ARP). A Transmission Control Protocol/Internet Protocol (TCP/IP) mechanism that maps a MAC address to an IP address in the ARP cache data structure. Defined in RFC 826. See also Neighbor Discovery Protocol (NDP).

adjacency. The relationship between neighboring devices for exchanging routing information. Adjacent devices share a common network segment.

A given device can have multiple adjacencies, but each adjacency consists of only two devices connected by one link. A protocol data unit (PDU) that goes between them does not have to pass through any other network devices. See also neighbor.

administrative distance. How reliable the source of the route is considered to be. A lower value is preferred over a higher value. An administrative distance of 255 indicates no confidence in the source; routes with this distance are not installed in the Routing Information Base (RIB). Also called route preference.

Advanced Encryption Standard (AES). A cryptographic algorithm for use by U.S. Government organizations to protect sensitive (unclassified) information. Defined in Federal Information Processing Standards (FIPS) PUB 197.

advertising. Process in which routing or service updates are sent at specified intervals so that other devices on the network can maintain lists of usable routes.

Agent Extensibility (AgentX). A protocol used to implement Simple Network Management Protocol (SNMP) that defines communications between an SNMP agent and an SNMP client. AgentX does not directly communicate with an SNMP client, but relies on the agent to handle the protocol details of SNMP. Defined by RFC 2741.

aggregate route. A single entry in a routing table that represents a combination of groups of routes that have common addresses. See also route summarization.

alarm indication signal (AIS). A signal transmitted instead of the normal signal to maintain transmission continuity and to indicate to the receiving device that a transmission interruption (fault) has occurred either at the equipment originating the AIS signal or upstream of that equipment.

American National Standards Institute (ANSI). A voluntary organization of corporate, government, and other members that develops international and U.S. standards relating to, among other things, communications and networking. ANSI is a member of the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO).

application-specific integrated circuit (ASIC). An integrated circuit that is designed for a specific application.

area. A logical division of devices that maintains detailed routing information about itself as well as routing information that allows it to reach other routing subdomains. An area divides a network into small, manageable pieces, reducing the amount of information each device must store and maintain about all other devices.

In Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF), an area is a set of contiguous networks and hosts within an autonomous system (AS) that have been administratively grouped together.

area border router (ABR). A router on the border of one or more Open Shortest Path First (OSPF) areas that connects those areas to the backbone network. An ABR is a member of both the OSPF backbone and its attached areas. Therefore, an ABR maintains routing tables for both the backbone topology and the topology of the other areas. See also Not-So-Stubby-Area (NSSA), stub area.

authentication. A process that verifies that data is not altered during transmission and ensures that users are communicating with the individual or organization that they believe they are communicating with.

authentication, authorization, and accounting (AAA). A framework for controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services:

- Authentication determines who the user is and whether to grant that user access to the network

- Authorization determines what the user can do
- Accounting tracks the user's activities and provides an audit trail that can be used for billing or resource tracking

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

Authentication Header (AH). An Internet Protocol Security (IPsec) protocol that authenticates either all or part of the contents of a packet by adding a header with a a hash message authentication code (HMAC) calculated based on the values in the packet. AH provides authentication but not confidentiality. See also Encapsulating Security Payload (ESP).

Automatic Protection Switching (APS). A means to detect a signal failure or signal degrade on a working channel and switch traffic to a protection channel. There are two types of APS:

- Ethernet Linear Protection Switching (ELPS)
- Ethernet Ring Protection Switching (ERPS)

autonomous system (AS). A network controlled as a single administrative entity sharing a common routing strategy. An autonomous system is subdivided into areas. An AS runs an Interior Gateway Protocol (IGP) such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Intermediate System to Intermediate System (IS-IS) within its boundaries. An AS uses an Exterior Gateway Protocol (EGP) to exchange routing information with other ASs.

autonomous system border router (ASBR). An area border router (ABR) located between an Open Shortest Path First (OSPF) autonomous system (AS) and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as Routing Information Protocol (RIP).

An ASBR is a link between the OSPF autonomous system and the outside network. An ASBR exchanges routing information with routers in other ASes. The ASBR redistributes routing information received from other ASs throughout its own AS. An ASBR must reside in a standard OSPF area.

availability. The amount of time that a system is available during time periods when it is expected to be available. Availability is often measured as a percentage of an elapsed year. For example, 99.95% availability equates to 4.38 hours of downtime in a year (0.0005 * 365 * 24=4.38) for a system that is expected to be available all the time.

B

B-MAC. A source and destination backbone MAC address (B-AA and a B-DA) in a Provider Backbone Bridging (PBB) header.

B-TAG. See backbone VLAN (B-VLAN).

backbone. The part of a network used as the primary path for transporting traffic between network segments.

backbone core bridge (BCB). A device that bridges frames based on backbone VLAN (B-VLAN) and backbone MAC address (B-MAC) information in a Provider Backbone Bridging (PBB) network core.

backbone edge bridge (BEB). A device that encapsulates customer frames for transmission across a Provider Backbone Bridging (PBB) network. There are two types:

- B-BEB (B type BEB): Contains a B-component for bridging in the provider space based on backbone MAC address (B-MAC) and backbone VLAN (B-VLAN) information.

- I-BEB (I type BEB): Contains an I-component for bridging in the customer space based on customer MAC address (C-MAC) and service VLAN (S-VLAN) information.

backbone VLAN (B-VLAN). A field in a Provider Backbone Bridging (PBB) header that carries the backbone VLAN identifier information. The format is the same as a service VLAN (S-VLAN) tag. Also called B-VID tag, B-TAG.

backhaul. The part of a hierarchical network that connects small subnetworks at the edge of the network to the core or backbone network.

In wireless backhaul, the part of the network that transports traffic from a cellular base station to a core network that routes and switches voice and data traffic.

bandwidth. A measure of the data transfer rate of a communications transport medium.

base station. An earth-based transmitting/receiving station for cellular phones and other wireless transmission systems.

Bellman-Ford algorithm. Used in distance-vector routing protocols such as Routing Information Protocol (RIP) to determine the best path to all routes in the network. Contrast with Dijkstra algorithm.

best effort. Traffic class in which the network forwards as many packets as possible in as reasonable a time as possible. By default, packets not explicitly assigned to a specific traffic class are assigned to the best-effort class.

BGP confederation. A method to solve scaling problems created by the iBGP full-mesh requirement. BGP confederations effectively break up a large autonomous system (AS) into subautonomous systems (sub-ASs). Each sub-AS must be uniquely identified within the confederation AS by a sub-AS number.

Within a sub-AS, the same iBGP full mesh requirement exists. Connections to other confederations are made with eBGP, and peers outside the sub-AS are treated as external. To avoid routing loops, a sub-AS uses a confederation sequence, which operates like an AS path but uses only the privately assigned sub-AS numbers.

BGP neighbor. Another device on the network that is running Border Gateway Protocol (BGP). There are two types of BGP neighbors: internal neighbors in the same autonomous system (AS) and external neighbors in different autonomous systems.

BGP peer. A remote Border Gateway Protocol (BGP) speaker that is an established neighbor of the local BGP speaker. BGP peers do not have to be directly connected to each other to share a BGP session.

BGP speaker. A router configured to run the Border Gateway Protocol (BGP) routing protocol. A BGP speaker must be explicitly configured with a set of BGP peers with which it exchanges routing information.

Bidirectional Forwarding Detection (BFD). Protocol that reduces the reliance upon the relatively slow hello mechanism in routing protocols to detect failures where no hardware signaling is available. BFD works with Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) v2, and Intermediate System to Intermediate System (IS-IS) to enable them to receive failure notifications. Defined in RFCs 5880 and 5881.

bit error rate (BER). The ratio of error bits to the total number of bits transmitted. A BER is generally shown as a negative exponent (for example, 10-7, which means one out of 10,000,000 bits is in error).

Border Gateway Protocol (BGP). An Exterior Gateway Protocol (EGP) that maintains a table of IP networks, or prefixes, which designate network reachability among autonomous system (AS) instances. BGP uses path-vector routing that makes decisions based on path, network policies, and/or rule sets. BGP is the primary protocol for the global Internet. First defined by RFC 1163.

BGP Version 4 (BGP4) defined in RFC 4271 supports Classless Interdomain Routing (CIDR) and route summarization.

BGP performs these tasks:

- Collects information about reachable networks from neighboring autonomous systems
- Advertises its reachable networks to routers inside the AS and to neighboring autonomous systems
- Selects routes if there are multiple routes available.

Each BGP device can have both external and internal connections to other BGP devices:

- Internal BGP (iBGP) connections are within the same autonomous system
- External BGP (eBGP) connections are between different autonomous systems

The configuration and behavior is slightly different between eBGP and iBGP.

You can use iBGP for multihomed BGP networks (with more than one connection to the same external autonomous system).

To avoid routing loops, iBGP does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full-mesh requirement becomes difficult to manage. To combat scaling problems, BGP uses route reflection and BGP confederations.

Multiprotocol BGP (MP-BGP) allows different types of addresses (address families) to be distributed in parallel. MP-BGP supports IPv4 and IPv6 addresses as well as unicast and multicast variants of each. Defining a neighbor under a particular address family means that you want to exchange routes from the particular address family with that neighbor. Defined in RFC 4760. See also IPv6 Provider Edge (6PE).

See also BGP neighbor, BGP peer, BGP speaker, community.

bridge. A device operating at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model that forwards frames from one network segment to another based on the MAC address.

The term bridge also describes a device that connects collision domains. Collisions that appear on one side of a switch are not allowed to propagate to the other.

Originally, bridges only had two ports, with each one connected to a network segment. Later, bridges had multiple ports that could connect more than two network segments as well as directly connecting hosts. As bridges evolved, they were also able to filter frames, that is, forward only certain traffic from one network segment to another. This type of device is sometimes called an intelligent bridge, but the more modern term is switch. The term “bridge” is somewhat archaic but is still often used in standards documents.

bridge protocol data unit (BPDU). A protocol data unit (PDU) sent by switches running the Spanning Tree Protocol (STP) to learn about other switches in the network and maintain the spanning tree.

broadcast. The process of a single host simultaneously sending the same message to all nodes on a network. Compare to multicast, where a only a subset of the receivers are addressed. See also unicast.

Broadcast, Unknown unicast, and Multicast (BUM). A generic term for three types of Ethernet frames that must be flooded and are major scaling challenges in Layer 2 (L2) data center networks, creating single-failure domains.

bursty. The tendency of the bandwidth needed in a network to vary greatly from one moment to the next.

C

C-MAC. A source and destination customer MAC address (C-SA and a C-DA) in a Provider Backbone Bridging (PBB) header.

C-TAG. See customer VLAN (C-VLAN).

Carrier Ethernet. Extensions to Ethernet that enable network operators to provide Ethernet services to customers and to use Ethernet technology in their networks. See also Metro Ethernet Forum (MEF).

certificate. Electronic document that identifies a person or entity. Through the use of keys and certificates, the entities exchanging data can authenticate each other.

channel. A connecting path that carries information from a sending device to a receiving device. A channel can refer to a physical medium (such as a coaxial cable or fiber optic cable).

circuit. A communications channel or path between two devices capable of carrying electrical current.

circuit switching. A network where a dedicated circuit must be opened between devices before they can communicate and, while the circuit is open, no other devices may use that circuit or parts of it. A circuit can remain open without any information transmission, and still be unusable by other devices; it must be closed before it is available to other users. Contrast with packet switching.

Class of Service (CoS). A way of managing traffic in a network by grouping similar types of traffic (for example, e-mail, video, voice, file transfer) together and treating each type as a class with its own level of service priority. However, no guarantees are made that a given priority will meet any specified minimum level. See also Quality of Service (QoS).

classful IP addressing. An older addressing scheme for configuring the ratio of networks to hosts using fixed length prefixes. See Classless Interdomain Routing (CIDR).

Classless Interdomain Routing (CIDR). A notation for specifying an IP addresses and its network prefix which appends a slash character to the address and a decimal number indicating the leading bits in the network prefix. For example:

- In the IPv4 notation “192.168.0.0/16”:
  - “192.168” (the first 16 bits) defines the network address.
  - .0.0 up to .255.255 refer to the host addresses on that network. This leaves 16 bits to contain host addresses, enough for 65536 host addresses.
- In the IPv6 notation “2001:db8::/32”:
  - “2001:db8” (the first 32 bits) defines the network address.
  - :0:0:0:0:0:0 to:ffff:ffff:ffff:ffff:ffff:ffff refer to host addresses on that network. This leaves 96 bits to contains host addresses, enough for 7,922,816,251,426,433 host addresses.

The lower the number after the slash, the more hosts contained in that block.

CIDR uses variable length subnet masking (VLSM) based on arbitrary length prefixes. In VLSM, the number of network and host bits assigned to a subnet can vary based on the number of hosts the subnet needs to support.

CIDR replaced traditional classful IP addressing, in which address allocation was based on octet (8-bit) boundary segments of the IP address. In CIDR, the boundary between the network and host portions of an IP address can be on any bit boundary. The old classful A, B, and C network designations correspond to CIDR prefixes of /8, /16, or /24. 192.168.0.0/16 corresponds to an old class B network. With CIDR, finer grained division of networks are possible, down to individual IP addresses, such as 192.168.100.2/32.

CIDR routes can be carried by Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), and Routing Information Protocol (RIP).

Before CIDR notation, IPv4 networks were represented using dotted decimal notation for both the address and a subnet mask.

Also called route summarization or supernetting.

client/server architecture. A computing architecture that distributes processing between clients and servers on the network. A client program makes a service request from a server which fulfils the request.

collapsed core. Collapsing the core layer and the distribution layer into one layer (one device) in the network design model. A collapsed core design reduces cost, while maintaining most of the benefits of the network design model for small networks that do not grow significantly larger over time.

collision domain. A network segment where data frames can collide with one another when being sent on a shared medium such as Ethernet. Hosts in a collision domain arbitrate among themselves using an access control mechanism.

command-line interface (CLI). Environment for entering commands to configure and monitor routing and switching software and hardware.

committed information rate (CIR). The average rate at which packets are admitted to the network. Each packet is counted as it enters the network. Packets that do not exceed the CIR are marked green, which corresponds to low loss priority. Packets that exceed the CIR but are below the peak information rate (PIR) are marked yellow, which corresponds to medium loss priority.

common and internal spanning tree (CIST). A single topology connecting all Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP) switches into one active topology. In other words, an entire spanning tree fabric.

common spanning tree (CST). The topology connecting all Spanning Tree Protocol (STP)/Rapid Spanning Tree Protocol (RSTP) *switches* and multiple spanning-tree (MST) region *instances*. An MST region appears as a single switch to spanning tree configurations outside the region.

community. In Border Gateway Protocol (BGP), a logical group of prefixes or destinations that share a common attribute; used to simplify a routing policy. Community members can be on different networks and in different autonomous systems.

In Simple Network Management Protocol (SNMP), an authentication scheme that authorizes SNMP clients based on the source IP address of incoming SNMP packets, defines which Management Information Base (MIB) objects are available, and specifies the operations (read-only or read-write) allowed on those objects.

congestion. The state in which the network load exceeds the available resources such as link capacity or memory buffers.

connection-oriented. A packet switching technology where a virtual circuit between sending and receiving devices makes it seem like the devices are connected by a switched circuit with a fixed bandwidth without regard to their physical addresses. In a connection-oriented service, packets always reach their destination in the same order as they were sent. Transmission Control Protocol (TCP) is a connection-oriented transport service. See also connectionless.

Connection-oriented protocols can be used to send information that requires a constant delay and bandwidth such as voice and video.

connectionless. A packet switching technology where the source and destination addresses are included in each packet so that a direct connection or an established session between sender and receiver is not required for communications. In a connectionless service, each packet is handled independently of all others, and packets might not reach their destination in the same order in which they were sent. User Datagram Protocol (UDP) is a connectionless transport service. See also connection-oriented.

Connectivity Fault Management (CFM). An Operation, Administration, and Maintenance (OAM) protocol that can manage Ethernet services and detect, verify, and isolate connectivity failures in VLANs. CFM enables service providers to configure:

- Maintenance association End Point (MEP) on a per-port, per-VLAN, or per-domain basis
- Maintenance domain Intermediate Point (MIP) on a per-port and per-level basis

CFM can operate over a LAN segment, customer VLAN (C-VLAN), service VLAN (S-VLAN), backbone VLAN (B-VLAN), or backbone identified by an I-SID (Service Instance Identifier). Defined by IEEE 802.1ag and 802.1ah.

Constrained Shortest Path First (CSPF). An extension of shortest path first (SPF). The path computed using CSPF is the shortest path that fulfills a set of constraints. After running the shortest path algorithm, the paths are pruned, removing those links that violate a given set of constraints.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Content Addressable Memory (CAM). An integrated circuit in a device that stores a table used to make frame forwarding and classification decisions. CAM can perform a massively parallel search of entries in the table much faster than a serial search than in conventional Random Access Memory (RAM).

There are two types of CAM:

- Binary CAM: A binary lookup that returns either a 1 or 0. A MAC address in an Ethernet frame comes into a switch, the switch looks in its MAC address table and either finds that MAC address or does not (1 or 0).
- Ternary CAM (TCAM): A binary lookup that returns either a 1 or 0 but also has a “do not care” bit. TCAM can have multiple matches and can determine a best match. This is necessary because Classless Interdomain Routing (CIDR) lookups need a longest prefix match. For example, 192.168.1.7/32 matches both 192.168.1.0/24 and 192.168.1.0/25. The closest match to 192.168.1.7/32 is 192.168.1.0/25 which would be chosen.

Continuity Check Message (CCM). A multicast Connectivity Fault Management (CFM) protocol data unit (PDU) transmitted periodically by a Maintenance association End Point (MEP) in ensure continuity over the Maintenance Association (MA) to which the transmitting MEP belongs.

control plane. The part of switch or router architecture that makes decisions about where traffic is sent. Control plane processing is the “signalling” of the network. Anything that is needed to get routing and switching working on a device is considered part of the control plane. The control plane serves the data plane.

The control plane functions include the manual system configuration and management operations performed by a network administrator. The control plane functions also include dynamic routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), or Border Gateway Protocol (BGP) that exchange topology information with other routers and construct a Routing Information Base (RIB).

The control plane functions are not performed on each arriving individual packet, so they do not have a strict speed constraint and are not time-critical.

Control plane packets are sent to or are locally originated by the device itself.

convergence. The synchronization process that a network must go through immediately after a topology change. Convergence time is the time required to update all the devices on the network with the routing information changes. See also routing table.

core layer. In the network design model, the layer that provides a transit function to access the internal network and external networks. The core layer moves packets between distribution layer devices. The core layer also links to the devices at the enterprise edge to support Internet, virtual private networks (VPN), extranet, and WAN access.

The core layer uses Layer 3 (L3) routing protocols that scale well and converge quickly such as Open Shortest Path First (OSPF).

The core serves as the backbone for the network and is critical for connecting distribution layer devices, so it is important for the core to be fast with low-latency, reliable, and scalable.

Also called backbone or trunk.

count-to-infinity. A distance-vector routing problem where if A tells B that it has a path somewhere, there is no way for B to know if the path has B as a part of it.

The count-to-infinity problem is caused by a link failure that partitions the network into two or more segments. When the network is partitioned, devices in one part of the segment cannot reach devices in the other part of the segment. The distance-vector algorithm adjusts the distance value slowly upwards toward infinity.

The count-to-infinity problem can be solved through split horizon methods.

cryptography. Rendering information unintelligible and restoring encrypted information to an intelligible form.

customer edge (CE). A device that provides an interface between a Local Area Network (LAN) and an enterprise or service provider core network. Outbound packets from the LAN are forwarded from the CE to a provider edge (PE) device, and inbound packets are forwarded from the PE to the CE.

customer VLAN (C-VLAN). In a Provider Bridging (PB) frame, a field that identifies the customer VLAN. See also service VLAN (S-VLAN). Also called C-TAG.

D

daemon. A background program that runs unattended and is usually invisible to users and that provides important system services. Pronounced “dee-mon” or “day-mon”.

Data Center Bridging (DCB). A collection of extensions for Ethernet that allows LANs and Storage Area Networks (SANs) to use a single unified fabric in a data center. DCB can carry Fibre Channel, TCP/IP, and inter-process communication traffic over a single, converged Ethernet network. DCB features include:

- Priority-based Flow Control (PFC)
- Enhanced Transmission Selection (ETS)
- Quantized Congestion Notification (QCN)
- Data Center Bridging Capability Exchange (DCBX)

Data Center Bridging Capability Exchange (DCBX). Defined in IEEE 802.1Qaz, a protocol that uses Link Layer Discovery Protocol (LLDP) to convey configuration of Data Center Bridging (DCB) features between neighbors.

data communications equipment (DCE). The interface between data terminal equipment (DTE) and a network.

Data Encryption Standard (DES). A method of data encryption using a private (secret) key. There are 72 quadrillion or more possible encryption keys that can be used. For each given message, the key is chosen at random from among these. Both the sender and the receiver must know and use the same private key.

In triple DES (3DES), a symmetric-key block cipher applies the DES cipher algorithm three times to each data block.

data link layer. See Layer 2 (L2).

data plane. The part of switch or router architecture that forwards frames and packets arriving on an interface. Routers and switches use what the control plane has built to process incoming frames and packets. The data plane forwards traffic to the next hop along the path to the destination according to the control plane logic. Data plane frames

or packets go *through* the device.

Also called forwarding plane.

data terminal equipment (DTE). Any device such as a host, router, or switch connected to a network. A DTE connects to a network through data communications equipment (DCE).

default gateway. A router that connects hosts on a network segment to the Internet.

default route. A route used to forward Internet Protocol (IP) packets when a more specific route is not present in the Routing Information Base (RIB). Often represented as 0.0.0.0/0, the default route is sometimes called the “route of last resort”.

Differentiated Services (DiffServ). A mechanism to classify and manage network traffic and provide Quality of Service (QoS) guarantees for service providers. DiffServ extends the Resource Reservation Protocol—Traffic Engineering (RSVP-TE). DiffServ enables traffic to be prioritized by class, so that certain kinds of traffic, for example voice traffic, can take precedence over other types of traffic.

DiffServ redefines bits in the type of service (ToS) field of an IP packet header. DiffServ uses the Differentiated Services Code Point (DSCP) field for the QoS priority and supports 64 levels of classification.

Defined by RFC 2474; Multi-Protocol Label Switching (MPLS) support is defined in RFCs 3270 and 4124.

Differentiated Services Code Point (DSCP). A six-bit field in an IP header that enables service providers to allocate resources on a per-packet basis to meet customer requirements. See also Differentiated Services (DiffServ).

Diffie–Hellman. A method of securely exchanging cryptographic keys that allows two parties with no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Digital Signature Algorithm (DSA). An asymmetric cryptographic algorithm that produces a digital signature in the form of a pair of large numbers. The signature is computed using rules and parameters such that the identity of the signer and the integrity of the signed data can be verified.

Dijkstra algorithm. An algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on link state. Also called shortest path first (SPF). Contrast with Bellman-Ford algorithm.

distance-vector routing. A family of routing algorithms that calculate the best route to use to send data based on information from adjacent (directly connected) routers on the network.

“Distance-vector” means that routes are advertised with two characteristics:

- Distance: How far it is to the destination based on a metric such as the number of hops, cost, bandwidth, or delay.
- Vector: The direction (exit interface) of the next hop router to reach the destination.

Each router sends its neighbors a list of networks it can reach and the distance to that network. For each network path, the receiving router picks the neighbor advertising the lowest metric, then adds this entry into its Routing Information Base (RIB). These best paths are advertised to each adjacent router.

Routing information is broadcast periodically rather than only when a change occurs, which makes the method compute- and bandwidth-intensive. For this reason, a distance-vector algorithm is best used in relatively small networks with few interrouter connections.

The Bellman-Ford algorithm is often used to determine the best path, which is used by the Routing Information Protocol (RIP).

Distance-vector routing can be prone to routing loops which are avoided through split horizon techniques.

Contrast with link-state routing and shortest-path routing.

distribution layer. In the network design model, the layer that aggregates the data received from the access layer and sends it to the core layer or to other segments of the local network. Routers or multilayer switches in the distribution layer performs many functions including:

- Routing between subnetworks and Virtual Local Area Network (VLAN) instances in the access layer
- Managing access control, routing, filtering, and QoS policies
- Managing firewalls and network address translation (NAT)
- Managing queues and prioritizing traffic
- Summarizing routes before advertising them to the core
- Isolating the core from access layer failures or disruptions

The distribution layer uses Layer 3 (L3) routing to connect to the core layer and Layer 2 (L2) switching to connect to the access layer.

Also called the aggregation layer or concentration layer.

domain. A representation of all or a subset of a network used for addressing and administrative purposes. Also refers to a collection of routers that use a common Interior Gateway Protocol (IGP). See also area and autonomous system (AS).

domain name. A meaningful and easy-to-remember name for an IP address. A domain name is a sequence of names (labels) separated by periods such as “ipinfusion.com”.

Domain Name Service (DNS). A service that translates a domain name into a numeric IP address needed to locate devices. The DNS database is hierarchical. When a client such as a Web browser gives a request that specifies a host name, the DNS resolver on the client first contacts a DNS server to determine the server's IP address. If the DNS server does not contain the needed mapping, it forwards the request to a different DNS server at the next higher level in the hierarchy. After potentially several forwarding and delegation exchanges within the DNS hierarchy, the IP address for the given host eventually arrives at the client. Defined in RFCs 1034 and 1035.

dotted decimal. A method of representing an IPv4 address as four decimal numbers separated by dots, or periods; for example, 194.65.87.3. See also IP address.

double colon. A notation used to represent a consecutive block of zeroes in the middle of an IPv6 address. For example, given this address:

FE80:0000:0000:0000:0202:B3FF:FE1E:8329

With double colon notation, the address shown above becomes:

FE80::0202:B3FF:FE1E:8329

You can only use the double colon notation once in an address.

double tagged. See Provider Bridging (PB).

dynamic address. An address assigned to a device on a network with no regard to matching a specific address to that device. When a client device (such as a laptop) is given a dynamic address, it simply receives one from a pool of available addresses. It might or might not be allocated the same IP address as on previous connections. See also Dynamic Host Configuration Protocol (DHCP).

Dynamic Host Configuration Protocol (DHCP). A protocol where a client can obtain an IP address and other information such as default gateway, subnet mask, and Domain Name Service (DNS) servers, for the client to use to

connect to a network. Defined in RFCs 2131 and 3315. See also Transmission Control Protocol/Internet Protocol (TCP/IP).

A DHCP server “leases” an IP address for a predetermined period of time, and reclaims the address for reassignment at the expiration of that period. DHCP greatly simplifies the administration of large networks, and networks in which nodes such as laptops, tablets, and smart phones frequently join and leave.

dynamic routing. A technique used by routing protocols where devices send and receive messages about the network topology to and from other devices and update a local Routing Information Base (RIB) used to locate the best available path to a destination.

There are different forms of dynamic routing: distance-vector routing, link-state routing, and path-vector routing. Several protocols use dynamic routing such as Border Gateway Protocol (BGP), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).

Also called adaptive routing. Contrast with static routing.

E

east/west. The flow of traffic traversing a data center or cloud horizontally between servers. Contrast with north/south.

Edge Virtual Bridging (EVB). A mechanism that enables a virtual switch to send all traffic to an adjacent physical switch. This moves the forwarding decisions and network operations from the host CPU to the switch. EVB leverages the advanced management capabilities in access or aggregation layer switches. Defined by IEEE 802.1Qbg.

egress. Outbound or outgoing, referring to a protocol data unit (PDU) exiting a device. See also ingress.

encapsulation. The technique used by layered protocols in which a layer adds its own header information to the protocol data unit (PDU) from the layer above. As an example, in the Open Systems Interconnection (OSI) Reference Model, a PDU can contain a header for Layer 1 (L1), followed by a header for Layer 2 (L2), followed by a header for the Layer 3 (L3), followed by a header for the transport layer (Transmission Control Protocol (TCP), followed by data for the higher layers.

encryption. The process of encoding information in an attempt to make it secure from unauthorized access, particularly during transmission. The reverse of this process is known as decryption. Two main encryption schemes are in common use:

- Private (symmetrical) key: Using a private encryption key known to both the sender and the receiver of the information.
- Public (asymmetrical) key: Using a public key to encrypt and a private key to decrypt.

See also Data Encryption Standard (DES).

end-of-row switch. A chassis-based switch in a rack or cabinet at either end of the server row in a data center that connects to hundreds of servers in that row. Each cabinet in the row has cabling connecting 48 (or more) servers to the end-of-row switch. An end-of-row switch typically has redundant supervisor engines, power supplies, and overall better high availability characteristics than a Top-of-Rack (ToR) switch.

An end-of-row switch extends Layer 1 (L1) cabling topology from the switch to each rack, resulting in a smaller Layer 2 (L2) footprint and fewer Spanning Tree Protocol (STP) nodes in the topology.

Enhanced Transmission Selection (ETS). A protocol for assigning bandwidth to frame priorities. Defined in IEEE 802.1Qaz.

equal-cost multipath (ECMP). A forwarding mechanism for routing traffic along multiple paths of equal cost that ensures load balancing. The link-state routing protocols that use a cost-based metric such as Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) explicitly allow ECMP routing.

Encapsulating Security Payload (ESP). An Internet Protocol Security (IPsec) protocol that ensures confidentiality by encrypting IP packets. An encryption algorithm combines the data in a packet with a key to transform the packet into an encrypted form. At the destination, the packet is decrypted it using the same algorithm. ESP also ensures the integrity of a packet using a hash message authentication code (HMAC). ESP also supports an authentication scheme like that used in Authentication Header (AH), or can be used in conjunction with AH.

Ethernet. A specification for a LAN technology at Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model based on packetized transmissions between physical ports over a variety of electrical and optical media. Ethernet can transport several upper-layer protocols, the most popular of which is Transmission Control Protocol/Internet Protocol (TCP/IP). Ethernet standards are maintained by the IEEE 802.3 committee.

Ethernet uses a bus topology and CSMA/CD (Carrier Sense Multiple Access/Collision Detection) to resolve contention when two devices try to access the network at exactly the same time. Transmission speeds range from 10 Mbps, to Fast Ethernet at 100 Mbps, to Gigabit Ethernet at 1000 Mbps.

Ethernet Linear Protection Switching (ELPS). A type of Automatic Protection Switching (APS) that specifies these techniques:

- Linear 1+1 (One-plus-One) operates with either uni-directional or bi-directional switching; normal traffic is copied and fed to both working and protection transport entities
- Linear 1:1 (One-to-One) operates with bi-directional switching; normal traffic is transported either on the working transport entity or on the protection transport entity, using a selector bridge at the source

Defined by ITU-T G.8031.

Ethernet Local Management Interface (E-LMI). An Operation, Administration, and Maintenance (OAM) protocol for communications between two User-to-Network Interface (UNI) instances. E-LMI provides both UNI and Ethernet Virtual Connection (EVC) status information to customer edge devices. This information enables automatic configuration of customer edge operation based on the configuration. Defined by Metro Ethernet Forum (MEF) 16.

Ethernet Ring Protection Switching (ERPS). A type of Automatic Protection Switching (APS) that protects traffic in a ring topology by ensuring that no loops are within the ring. Loops are prevented by blocking traffic on either a predetermined link or a failed link. ERPS integrates Operation, Administration, and Maintenance (OAM) functions with a simple APS protocol. An Ethernet ring uses normal learning, forwarding, filtering, and flooding mechanisms and a forwarding database (FDB). Defined by ITU-T G.8032.

Ethernet to the First Mile (EFM). A set of extensions to the 802.3 MAC and MAC sub layer. EFM describes technologies and the physical layer specifications for subscriber access, including remote failure detection, remote loop back, and link monitoring. Defined by IEEE 802.3ah.

Ethernet Virtual Connection (EVC). An association of two or more instances of a User-to-Network Interface (UNI). There are three types of EVC:

- In a point-to-point EVC, exactly two UNIs are associated with one another.
- In a multipoint EVC, two or more UNIs are associated with one another.
- In a rooted-multipoint EVC, one or more of the UNIs must be designated as root and each of the other UNIs must be designated as a leaf. If root, the UNI can send service frames to all other points in the EVC; if leaf, the UNI can send and receive service frames to and from root only.

Explicit Route Object (ERO). An extension to Resource Reservation Protocol (RSVP) that allows a path message to traverse an explicit sequence of routers that is independent of conventional shortest-path IP routing.

Exterior Gateway Protocol (EGP). An interdomain protocol such as Border Gateway Protocol (BGP) used to exchange network reachability information between autonomous system (AS) instances. Contrast with Interior Gateway Protocol (IGP).

F

FEC-to-NHLFE (FTN) map. In Multi-Protocol Label Switching (MPLS), a mapping from the forwarding equivalence class (FEC) of incoming packets to the corresponding Next Hop Label Forwarding Entry (NHLFE).

filtering. The process of determining whether to forward a frame or packet through a port. The simplest form of filtering is to not forward frames out the same port on which they were received. A network administrator can configure filtering manually or a device can be "self-learning" and record the source addresses of devices on each segment of a network in a filtering database.

Filtering behavior is sometimes referred to as "drop, flood, or forward":

- If the switch determines that the destination MAC is on the same port, it does not forward the frame, dropping it.
- If the switch determines that the destination MAC is on a different port, it forwards the frame on that port.
- If the switch does not know where to send the frame (or if it is multicast or broadcast), the frame is flooded out all ports (except the port it was received on).

filtering database. A data structure in a switch that maps addresses to ports, addresses to VLANs, and/or ports to VLANs. A switch learns the location of hosts by recording the source MAC address-port number association for each frame received at an incoming port. All future transmissions destined to a MAC address in the filtering database are only directed to the port associated with that MAC address unless the transmission originated on that port.

A switch can also be configured and act as several independent switches by creating VLAN associations to switch ports.

flapping. Condition of network instability when a route is announced and then withdrawn repeatedly, usually as the result of an intermittently failing link. Also called route flapping.

flooding. Forwarding a frame onto all ports except the port upon which it arrived. In Open Shortest Path First (OSPF), distributing and synchronizing the link-state database (LSDB) between routers.

flow control. Any mechanism that prevents a source from sending faster than the destination is capable of receiving.

Forward Error Correction (FEC). A system of error control that allows the receiver to correct some errors without having to request a re-transmission of data.

forwarding. Finding the output port to which a frame needs to go, and relaying the frame to that port.

forwarding equivalence class (FEC). A set of packets with similar characteristics that are forwarded in the same manner, on the same path, with the same forwarding treatment, and using the same Multi-Protocol Label Switching (MPLS) label. FECs are defined by the Label Distribution Protocol (LDP). FECs are also represented in other label distribution protocols.

Forwarding Information Base (FIB). A data structure used to find the interface to which to forward a packet. The FIB contains the minimum amount of information required to make a forwarding decision for a particular packet, such

as destination prefix and nexthop. The FIB is an abbreviated form of the information in the Routing Information Base (RIB).

Also called forwarding table.

frame. A protocol data unit (PDU) at Layer 2 (L2) with addressing and protocol control information. A frame contains a header field and a trailer field that "frame" the user data. (Some control frames contain no data.)

See also packet.

G

GARP Multicast Registration Protocol (GMRP). A Generic Attribute Registration Protocol (GARP) application that allows switches to exchange multicast group information with other GMRP switches, prune unnecessary broadcast traffic, and dynamically create and manage multicast groups. See also Multiple MAC Registration Protocol (MMRP).

GARP VLAN Registration Protocol (GVRP). A Generic Attribute Registration Protocol (GARP) application that provides VLAN registration services. A switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLANs. Defined by 802.1Q. See also Multiple VLAN Registration Protocol (MVRP).

gateway. A device that understands and converts between two different networking models. Since Transmission Control Protocol/Internet Protocol (TCP/IP) has become the dominant model, gateways are not used much at this time.

See also default gateway.

Generic Attribute Registration Protocol (GARP). A generic framework for devices to register attributes, such as VLAN identifiers and multicast group membership. See also Multiple Registration Protocol (MRP).

generic routing encapsulation (GRE). A tunneling protocol that encapsulates Layer 3 (L3) packets inside IP packets. GRE provides a virtual point-to-point link over an IP network. GRE is completely insecure, but provides a fast and simple way to access a remote network.

graceful restart. A process that allows a router whose control plane is restarting to continue forwarding traffic while recovering its state from neighboring routers. Without graceful restart, a control plane restart disrupts services provided by the router. Also called nonstop forwarding.

gratuitous ARP. Broadcast request for a router's own IP address to check whether that address is being used by another node. Used to detect IP address duplication.

H

hash message authentication code (HMAC). A method of calculating a message authentication code (MAC) using a cryptographic hash function in combination with a secret cryptographic key. As with any MAC, it can be used to simultaneously verify both the data integrity and the authenticity of a message. Any cryptographic hash function, such as MD5 or SHA-2, can be used to calculate an HMAC.

header. The portion of a protocol data unit (PDU) that contains control information for the message such as destination address, source address, input sequence number, the type of message, and priority level.

hello packet. A multicast packet that is used by protocols for neighbor discovery and recovery. Hello packets also indicate that a client is still operating and network-ready.

high availability. The ability of a system or component to limit or avoid network disruption when a component fails. High availability provides both hardware and software methods to minimize downtime and improve the performance of a network.

hold down. A state that a route is placed into so that devices will neither advertise the route nor accept advertisements about the route for a specific length of time (the hold down period). A hold down is used to flush bad information about a route from all devices in a network. A route is placed into hold down when a link in that route fails.

hop. A single link between two computer systems that a protocol data unit (PDU) must cross on its way to its destination. See also hop count.

hop count. The number of links that must be crossed to get from a source to a destination. A protocol data unit (PDU) might pass over many hops to reach its destination. If it must pass between five computers, it is said to have taken four hops to reach its destination. Hop count is often used as a metric for evaluating a route in distance-vector routing. Routing Information Protocol (RIP) uses hop count as its sole metric.

host. A computer connected to a network that is assigned a Layer 3 (L3) address and that provides an access point to that network. Similar to a node, except that host usually implies a computer system, whereas node generally applies to any networked device such as a router or switch.

hypervisor. A thin operating system designed solely to provide virtualization. A hypervisor drives physical hardware, executes virtual machine (VM) instances, and dynamically shares the underlying hardware with the associated virtual hardware. A hypervisor does not serve as a general-purpose operating system, but instead provides the platform on which VMs can run.

I

I-SID (Service Instance Identifier). A field in an I-TAG that defines the service instance to which the Provider Backbone Bridging (PBB) frame is mapped.

I-TAG. Field in the Provider Backbone Bridging (PBB) header that carries the I-SID (Service Instance Identifier) associated with the frame.

Incoming Label Map (ILM). In Multi-Protocol Label Switching (MPLS), a mapping from incoming labels to corresponding Next Hop Label Forwarding Entry (NHLFE).

ingress. Inbound or incoming, referring to a protocol data unit (PDU) entering a device. See also egress.

Institute of Electrical and Electronics Engineers (IEEE). A coordinating body for computing and communications standards. The IEEE mainly covers Layer 1 (L1) and Layer 2 (L2) of the Open Systems Interconnection (OSI) Reference Model. (Pronounced “eye-triple-ee”.) See http://www.ieee.org.

interface. The point at which a connection is made between two devices. An interface describes the logical and physical connections and usually means the same thing as the term port.

Interior Gateway Protocol (IGP). An intradomain protocol used to exchange network reachability and routing information among devices within an autonomous system (AS), such as Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF), or Routing Information Protocol (RIP). Contrast with Exterior Gateway

Protocol (EGP).

Intermediate System to Intermediate System (IS-IS). An Interior Gateway Protocol (IGP) that floods link state information throughout a network of routers. Each IS-IS router independently builds a database of the network's topology, aggregating the flooded network information. A Routing Information Base (RIB) is calculated from the database by constructing a shortest path tree (SPT).

Like Open Shortest Path First (OSPF), IS-IS uses the Dijkstra algorithm to find the best path through a network. Packets are then forwarded, based on the computed ideal path, through the network to the destination.

Defined by International Organization for Standardization (ISO) 10589.

internal spanning tree (IST). A special type of multiple spanning-tree instance (MSTI) that runs in an multiple spanning-tree (MST) region. An IST connects all the switches in the MST region and appears as a subtree in the common and internal spanning tree (CIST) that encompasses the entire switched domain.

An IST is identified by the number zero (0) and exists on all ports; you cannot delete the IST. By default, all VLANs are assigned to the IST. The IST is the only spanning tree instance that sends and receives bridge protocol data unit (BPDU) messages.

Any other spanning tree instance within an MST region is called a multiple spanning-tree instance (MSTI).

International Organization for Standardization (ISO). An international standards body that establishes global standards for communications and information exchange. Voting members are designated standards bodies of participating nations; American National Standards Institute (ANSI) is the U.S. member of the ISO. The Open Systems Interconnection (OSI) Reference Model is one of the ISO's most widely accepted recommendations.

Sometimes mistakenly referred to as the "International Standards Organization". Because "International Organization for Standardization" has different acronyms in different languages (IOS in English, OIN in French for *Organisation internationale de normalisation*), the founders gave it the short form ISO. ISO is derived from the Greek *isos*, meaning "equal".

For more, see http://www.iso.org/iso/home.html.

International Telecommunication Union (ITU). An international organization that develops standards for telecommunications. Formerly known as the CCITT. See http://www.itu.int.

Internet. The world's largest computer network, serving universities, commercial interests, government agencies, and private individuals. The Internet uses Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, and Internet computers and devices run many different operating systems.

No government agency, single person, or corporate entity controls the Internet. All decisions on methods and standards are made by standards groups based on input from users.

See also Internet Engineering Task Force (IETF); Request for Comments (RFC).

Internet Control Message Protocol (ICMP). An Internet Protocol (IP) that provides management and control functions. Routers send ICMP messages to respond to undeliverable datagrams by placing an ICMP message in an IP datagram and then sending the datagram back to the original source. ICMP is also used by the ping (packet internet groper) command and enables a host to discover addresses of operating routers on the subnet. Defined in RFC 792.

IPv6 makes greater use of ICMP (ICMPv6 defined in RFC 4443) than IPv4, including neighbor solicitation, neighbor advertisement, router solicitation, router advertisement, and redirect.

Internet Engineering Task Force (IETF). An international community of network designers, operators, vendors, and researchers that develops Request for Comments (RFC) documents that define protocols and specifications for the Internet. The IETF mainly covers Layer 2 (L2) and Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. See http://www.ietf.org.

Internet Group Management Protocol (IGMP). An IPv4 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3376.

IGMP enables receivers to register that they want to receive a particular multicast transmission, but does not route multicast traffic from the source to receivers. That task is left to a multicast routing protocol, such as Protocol Independent Multicast (PIM).

See also Multicast Listener Discovery (MLD), multicast group, (S,G).

Internet Key Exchange (IKE or IKEv2). An Internet Protocol Security (IPsec) protocol used to set up a security association (SA) by negotiating keys in secret. IKE builds upon Internet Security Association and Key Management Protocol (ISAKMP) using X.509 certificates for authentication and a Diffie–Hellman key exchange to set up a shared session secret from which cryptographic keys are derived. In addition, a security policy for every peer which will connect must be manually maintained.

The IKE protocol runs in two phases. The first phase establishes a ISAKMP SA which is used in the second phase to negotiate and set up the IPsec SAs.

Internet Protocol (IP). A Layer 3 (L3) protocol that provides connectionless delivery of data across heterogeneous physical networks. IP provides features for addressing, type-of-service, fragmentation and reassembly, and security. Defined by RFCs 791 and 1349.

Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it from all other computers on the Internet.

IP is best effort and provides no guarantees of reliability, so if packets are lost in transit, accidentally duplicated, arrive in the wrong order, or arrive corrupted, no effort is made to address the problem on the IP level—that is left to protocols a layer above, such as Transmission Control Protocol (TCP).

Internet Protocol Security (IPsec). A protocol suite for securing IP communications by authenticating and encrypting packets during a communication session. Authentication Header (AH) and Encapsulating Security Payload (ESP) are the main wire-level protocols used by IPsec. Before either AH or ESP can be used, however, the two devices must share a public key through Internet Key Exchange (IKE or IKEv2).

RFC 2401 specifies the base architecture for IPsec compliant systems. RFCs 2402, 2406, and 2407 provide more details about IPsec.

Internet Security Association and Key Management Protocol (ISAKMP). A framework for authentication and key exchange with actual authenticated keying material provided either by manual configuration with pre-shared keys or Internet Key Exchange (IKE or IKEv2). See also Internet Protocol Security (IPsec).

IP address. A unique number that identifies a device on an Internet Protocol (IP) network. IP addresses have two formats:

- An IPv4 address is 32 bits and is usually written in dotted decimal notation as four decimal numbers separated by periods. For example, 192.168.50.4 is an IPv4 address.
- An IPv6 address is 128 bits and is written in a hexadecimal notation of eight 16-bit parts separated by colons. For example, FE80:0000:0000:0000:0202:B3FF:FE1E:8329 is an IPv6 address. In the double colon address format, consecutive colons (“::”) represent successive 16-bit blocks that contain zeros: FE80::0202:B3FF:FE1E:8329. While a much larger address space is a feature, IPv6 also has other features such as multicast support, jumbograms (packets up to 4 GB in size), and stateless host auto-configuration.

Table 3-1 compares the IPv4 and IPv6 address formats.

Table 3-1: IPv6 and IPv4 Address Formats

Feature	IPv6	IPv4
Address space	128-bits = 3.4 x 1038 (340 unidecillion)	32-bits = 4.3 x 109 (4.2 billion)
Field separator	colon (:)	period (.)
Notation	hexadecimal	decimal
Example	db8:0:0:1	0.23.2.3

Each IP address contains a network part, an optional subnetwork part, and a host part. The network and subnetwork parts together are used for routing, while the host part is used to address an individual host within the network or subnetwork. A subnet mask is used to extract network and subnetwork parts from the IP address. Classless Interdomain Routing (CIDR) provides a way to represent IP addresses and subnet masks.

IP addresses are difficult to remember, so people tend to refer to computers by their domain names instead.

IPv6 Provider Edge (6PE). A protocol that enables IPv6 domains to communicate with each other over an Multi-Protocol Label Switching (MPLS) IPv4 core network. 6PE routers are “dual stack” and run both IPv4 and IPv6. Multiprotocol Border Gateway Protocol (BGP) (MP-BGP) in the IPv4 network is used to exchange IPv6 reachability information along with a label for each IPv6 prefix announced. Defined in RFC 4798.

Also called V6PE.

K

keepalive message. A message sent between devices when no data traffic has been detected for a given period of time. This communication verifies that the virtual and physical connection between the devices is still active.

kernel. The part of an operating system that performs basic functions such as allocating hardware resources.

KVM (Kernel-based Virtual Machine). A virtualization infrastructure for the Linux kernel that turns it into a hypervisor. KVM requires a processor with hardware virtualization technology extensions. By itself, KVM does not perform any emulation. Instead, KVM exposes an interface with which a user space host can then set up guest virtual machine (VM) instances.On Linux, QEMU (Quick EMUlator) is one such user space host.

L

Label Distribution Protocol (LDP). A protocol for distributing labels in non-traffic-engineered applications. LDP allows routers to create label-switched path (LSP) instances through a network by mapping network layer routing information directly to data-link layer switched paths.

A label is a short fixed-length, locally-significant identifier that identifies a forwarding equivalence class (FEC).

LDP works with other routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) to create LSPs.

See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

label edge router (LER). A router that operates at the edge of an Multi-Protocol Label Switching (MPLS) network and acts as the entry and exit points for the network.

When forwarding IP packets into an MPLS domain, an LER makes the initial path selection, add the appropriate labels to the packet, and forwards the labelled packets into the MPLS domain. Likewise, upon receiving a labelled packet which is destined to exit the MPLS domain, the LER strips off the label and forwards the resulting IP packet using normal IP forwarding rules. (Under penultimate hop popping (PHP), the popping function might be performed by an label switch router (LSR) directly connected to the LER.)

Also called an edge LSR.

label switch router (LSR). A Multi-Protocol Label Switching (MPLS) router located in the middle of a MPLS network. When an LSR receives a packet, it uses the label included in the packet header to determine the next hop on the label-switched path (LSP) and find a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is forwarded.

Also called transit router.

label-switched path (LSP). A sequence of routers that cooperatively perform Multi-Protocol Label Switching (MPLS) operations for a packet stream. An LSP is a unidirectional, point-to-point, half-duplex connection carrying information downstream from the ingress (first) router to the egress (last) router. The ingress and egress routers cannot be the same device.

latency. Delay in the transmission through a network from source to destination. See also line rate, wire speed.

Layer 1 (L1). The physical layer in the Open Systems Interconnection (OSI) Reference Model that conveys the bit stream through electrical impulse, light waves, or radio signals through the network. L1 represents the basic network hardware and specifies the type of medium used for transmission and the network topology.

Layer 2 (L2). The data link layer in the Open Systems Interconnection (OSI) Reference Model that provides reliable transit of data across a physical link between two directly connected devices. L2 refers to physical addressing, network topology, line discipline, error notification, sequenced delivery of frames, and flow control.

L2 transfers data between network entities by splitting data into frames to send on Layer 1 (L1) and receiving acknowledgment frames. The data link layer performs error checking and retransmits frames not received correctly. In general, the data link layer controls the flow of information across the link, providing an error-free virtual channel to Layer 3 (L3).

The data-link layer has two sublayers:

- logical link control (LLC)
- Media Access Control (MAC)

Also called link layer.

Layer 3 (L3). The network layer in the Open Systems Interconnection (OSI) Reference Model that routes packets of data from source to destination across a network. L3 provides network-wide communication, including global addressing, lifetime control, fragmentation, and reassembly. Internet Protocol (IP) is an example.

Layer 4 (L4). The transport layer in the Open Systems Interconnection (OSI) Reference Model that provides logical communication between processes running on different hosts. L4 manages the end-to-end delivery of payload from a source to a destination within and between networks while maintaining the quality of service. Transmission Control Protocol (TCP) is an example.

Lightweight Directory Access Protocol (LDAP). A protocol used to locate organizations, individuals, and other resources in a network. Defined in RFC 4511. See also authentication, authorization, and accounting (AAA), Remote Authentication Dial In User Service (RADIUS), Terminal Access Controller Access Control System Plus (TACACS+).

line rate. Total number of physically transferred bits per second, including useful data and protocol overhead, over a communication link. For example, if the line rate of a link is 10 Gbps, the link transmits 10 gigabits of data every second over its physical interface. Contrast with throughput. See also latency, wire speed.

link. Communication path between two neighbor nodes.

link aggregation. A method for using multiple parallel links between a pair of devices as if they were a single higher-performance channel. The aggregated interface is viewed as a single link to each device. Spanning Tree Protocol (STP) also views it as one interface. Link aggregation can also be used to increase availability so that when there is a failure in one physical link, the remaining links stay up, and there is no disruption. Defined by IEEE 802.1AX.

Also called link aggregation group (LAG), LAG bundle, and EtherChannel. See also Link Aggregation Control Protocol (LACP), Multi-Chassis Link Aggregation (MC-LAG).

Link Aggregation Control Protocol (LACP). Mechanism for exchanging port and system information to create and maintain link aggregation groups.

link cost. An arbitrary number configured on an Open Shortest Path First (OSPF) interface which is used in shortest path first calculations.

Link Layer Discovery Protocol (LLDP). A mechanism for the devices on a network to advertise their identity, capabilities, and neighbors to each other. Defined by IEEE 802.1AB.

link state. Information about a link and link cost to neighboring routers.

link-state advertisement (LSA). An Open Shortest Path First (OSPF) protocol data unit (PDU) to share information on the operating state of a link, link cost, and other OSPF neighbor information. LSAs are used by the receiving routers to update their Routing Information Base (RIB)s.

link-state database (LSDB). The data structure on a router that contains all routing knowledge in a link-state network. An LSDB stores all link-state advertisement (LSA) instances produced by a link-state routing protocol such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS). Each router runs shortest path first (SPF) algorithm against this database to locate the best network path to each destination in the network.

link-state routing. A routing technique used by Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) where each router shares information with other routers by flooding information about itself to every reachable router in the area. Link-state protocols use characteristics of the route such as speed and cost to determine the best path. Link-state information is transmitted only when something has changed in the network.

Every router constructs a map of the connectivity of the network, determining the interconnections between all routers. As a router receives an advertisement, it stores this information in a link-state database (LSDB). Each router then independently calculates the best next hop from it to every possible destination in the network using the shortest path first (SPF) algorithm to build a shortest path tree (SPT) with itself as the center of that tree. The shortest path to each reachable destination within the network is found by traversing the tree. The collection of best next hops forms the router's Routing Information Base (RIB).

Link-state algorithms create a consistent view of the network and are therefore not prone to routing loops, but they achieve this at the cost of more computing cycles and more traffic compared to distance-vector routing.

See also Dijkstra algorithm.

Linktrace Message (LTM). A Connectivity Fault Management (CFM) protocol data unit (PDU) initiated by a Maintenance association End Point (MEP) to trace a path to a target MAC address, forwarded from Maintenance domain Intermediate Point (MIP) to MIP, up to the point at which the LTM reaches its target MEP.

Linux. A Unix-like computer operating system assembled under the model of free and open source software development and distribution. The defining component of Linux is the kernel, the central part of the operating system that manages system services. Many people use the name “Linux” to refer to the complete operating system package which is called a Linux distribution which is made up of a collection of software based around the Linux kernel.

Linux has since been ported to more computer hardware platforms than any other operating system and is available for a wide variety of systems from small embedded systems up to supercomputers. In particular, networking devices such as switches and routers almost universally run some Linux distribution.

As an open operating system, Linux is developed collaboratively, meaning no one organization is solely responsible for its development or ongoing support. Companies participating in the Linux community share research and development costs with their partners and competitors.

Local Area Network (LAN). A group of computers and devices connected by a communications channel, capable of sharing resources among several users. LANs are based on a small physical area such as a building, floor, or department. LANs can connect to a wide area network (WAN). Ethernet is the most popular LAN technology.

logical link control (LLC). The higher sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The LLC sublayer provides the interface for Layer 3 (L3) and handles error control, flow control, framing, and MAC-sublayer addressing. The most prevalent LLC protocol is IEEE 802.2, which includes both connectionless and connection-oriented variants. See also Media Access Control (MAC).

loopback. A troubleshooting test in which a signal is transmitted from a source to a destination and then back to the source again so that the signal can be measured and evaluated.

M

MAC address. A permanent, unique serial number that uniquely identifies a network device among all other network devices in the world. MAC addresses are 12-digit numbers, 48 bits in length. MAC addresses are usually written as six groups of two hexadecimal digits, separated by hyphens (“-”) or colons (“:”):

MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Each pair of hexadecimal digits represents one byte of the 6-byte (48-bit) address.

An example of a MAC address is 68:A3:C4:3B:8D:24:

- The first three parts (68:A3:C4) identify the manufacturer (Liteon Technologies)
- The second three parts (3B:8D:24) is the serial number assigned by the manufacturer

At Layer 2 (L2), other devices use MAC addresses to locate specific ports in a network, and to create and update a Routing Information Base (RIB). A MAC address maps to an IP address through the Address Resolution Protocol (ARP).

Also called physical address, Ethernet address, or hardware address.

MAC-in-MAC. See Provider Backbone Bridging (PBB).

Maintenance Association (MA). In Connectivity Fault Management (CFM), a set of Maintenance association End Point (MEP) instances, each configured with the same MAID (Maintenance Association Identifier) and Maintenance Domain (MD) Level, established to verify the integrity of a single service instance.

Maintenance association End Point (MEP). A Connectivity Fault Management (CFM) entity at the edge of a Maintenance Domain (MD) that confines CFM messages within the domain via the MD level. MEPs periodically

transmit and receive Continuity Check Message (CCM) instances from other MEPs within the domain. MEPs are either “Up” (toward the switch) or “Down” (toward the wire).

Maintenance Domain (MD). In Connectivity Fault Management (CFM), the network or the part of the network for which faults in connectivity can be managed.

Maintenance domain Intermediate Point (MIP). A Connectivity Fault Management (CFM) entity that catalogs and forwards information received from Maintenance association End Point (MEP) instances. MIPs are passive points that respond only to CFM Linktrace Message (LTM) and loopback messages.

Management Information Base (MIB). A specification of objects used by Simple Network Management Protocol (SNMP) to monitor or change network settings. MIBs provides a logical naming scheme for resources on a network. A MIB contains information about a device such as settings, usage statistics, performance data, or physical properties (such as temperature or fan speed). MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches. Standard MIBs are defined by the IETF.

Maximum Transmission Unit (MTU). The maximum number of bytes in a packet or frame. For Ethernet, the default MTU is 1500 bytes (data payload), but each media has different sizes. The Ethernet MTU is defined in RFC 894.

Media Access Control (MAC). The lower sublayer of Layer 2 (L2) in the Open Systems Interconnection (OSI) Reference Model. The MAC sublayer provides addressing and channel access control mechanisms that make it possible for several network nodes to communicate within a multiple-access network that uses a shared medium such as Ethernet. The MAC sublayer is the interface between the logical link control (LLC) sublayer and Layer 1 (L1).

merchant silicon. Networking chips, usually ASICs, that are designed and made by an entity other than the company selling the switches in which they are used. The traditional approach to building network products is to design custom ASICs and supporting chips that completely focus on the features needed to deliver the product. The levels of expertise required to design and build such a chip requires specific skills, tools, and high levels of expertise. If your core business is producing a networking device, then by relying on companies who specialise in silicon design and manufacture, you can focus on software and integration to deliver features at a cheaper price.

mesh. A physical or logical network topology in which devices have many redundant interconnections. A full mesh is when all devices in a network have a connection to all other devices, a partial mesh is when some devices have a connection to all other devices.

Metro Ethernet Forum (MEF). A defining body for Carrier Ethernet with many participating organizations including service providers, and network hardware and software manufacturers. The MEF’s mission is to accelerate the worldwide adoption of carrier-class Ethernet networks and services. For more, see http://metroethernetforum.org/.

Multi-Chassis Link Aggregation (MC-LAG). A technique that extends the link aggregation concept. At either one or both ends of a link aggregation group, a single aggregation system is replaced by a *portal* that is a collection of one to three portal systems. Defined by IEEE 802.1AX.

Also called MLAG and Distributed Resilient Network Interconnect (DRNI).

Multi-Protocol Label Switching (MPLS). A method for forwarding packets through a network. MPLS operates between the traditional definitions of Layer 2 (L2) and Layer 3 (L3).

In a traditional IP network, each router performs an IP lookup to determine a next hop based on its routing table, and forwards the packet to that next hop. Every router in the path repeats this process, making its own independent routing decisions, until the final destination is reached.

In an MPLS network, the first device does a routing lookup, but instead of finding a next hop, it finds the final destination router and finds a pre-determined path from the source to the destination. The router applies a “label”

based on this information. Other routers in the path use the label to route the traffic without needing to perform any additional IP lookups.

At each incoming (ingress) point of the network, packets are assigned a label by a label edge router (LER). Packets are forwarded along an label-switched path (LSP) where each label switch router (LSR) makes forwarding decisions based on the label information. At each hop, an LSR swaps the existing label for a new label that tells the next hop how to forward the packet. At the outgoing (egress) point, an LER removes the label, and forwards the packet to its destination via IP routing.

MPLS enables these applications: Virtual Private Network (VPN), traffic engineering (TE), and Quality of Service (QoS).

See also Label Distribution Protocol (LDP), Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Multi-Protocol Label Switching - Transport Profile (MPLS-TP). A subset of Multi-Protocol Label Switching (MPLS) with extensions that address transport network requirements. The extensions provide the same QoS, protection and restoration, and Operation, Administration, and Maintenance (OAM) as in SONET/SDH. In MPLS-TP, some of the MPLS functions are turned off, such as penultimate hop popping (PHP), label-switched path (LSP) merge, and equal-cost multipath (ECMP).

The use of a control plane protocol is optional in MPLS-TP. The control plane can set up an LSP automatically across a packet-switched network domain. However, some network operators might prefer to configure the LSPs statically without using an IP or routing protocol.

multicast. The process of a single host sending messages to a selected group of receivers. See also broadcast, unicast.

multicast group. A collection of hosts receiving packets from a host that is transmitting multicast packets. Only hosts that need to hear a particular multicast declare that requirement. A multicast group restricts traffic to just those paths between the sources and destinations associated with the multicast address. Membership is dynamic; when a host joins a group, it starts receiving the datastream, and when a host leaves a group, it stops receiving the datastream. When there are no more members, the group simply ceases to exist.

See also GARP Multicast Registration Protocol (GMRP), Internet Group Management Protocol (IGMP), Multicast Listener Discovery (MLD), Multiple MAC Registration Protocol (MMRP), (S,G).

Multicast Listener Discovery (MLD). An IPv6 protocol that allows hosts to add or remove themselves from a multicast group. Defined by RFC 3810.

See also Internet Group Management Protocol (IGMP), multicast group, (S,G).

Multiple MAC Registration Protocol (MMRP). A protocol that manages multicast group MAC addresses. In addition, MMRP improves the convergence time of GARP Multicast Registration Protocol (GMRP). Defined by 802.1ak.

Multiple Registration Protocol (MRP). A generic registration framework with protocols, procedures, and managed objects for switches to register attributes with other switches in a LAN. Defined by 802.1ak. MRP replaces Generic Attribute Registration Protocol (GARP)

Multiple Spanning Tree Protocol (MSTP). An enhancement to the Rapid Spanning Tree Protocol (RSTP) where a separate spanning tree for can be configured for a VLAN group. Each VLAN group belongs to a multiple spanning-tree instance (MSTI). Several MSTIs can run in an multiple spanning-tree (MST) region, with each region interconnected in a common and internal spanning tree (CIST).

MSTP is backward compatible with both RSTP and Spanning Tree Protocol (STP).

Originally defined in IEEE 802.1s and later merged into 802.1Q.

multiple spanning-tree (MST) region. A collection of interconnected switches that have the same Multiple Spanning Tree Protocol (MSTP) configuration which includes region name, revision number, and VLAN-to-instance map. Each MST region can contain multiple instances of spanning trees. The network administrator must properly configure participating switches throughout the region. All regions are bound together using a common and internal spanning tree (CIST), which creates a loop-free topology across regions. An MST region appears as a single switch to spanning tree configurations outside the region.

multiple spanning-tree instance (MSTI). A group of VLANs in a spanning-tree instance managed by Multiple Spanning Tree Protocol (MSTP) within an multiple spanning-tree (MST) region. Within each MST region, MSTP maintains multiple spanning-tree instances. Each instance has a spanning-tree topology independent of other spanning-tree instances. An MSTI provides a fully connected active topology for frames belonging to a VLAN. You can assign a VLAN to only one spanning-tree instance at a time.

An internal spanning tree (IST) is a special type of MTSI.

Multiple VLAN Registration Protocol (MVRP). A protocol that manages registration of VLANs, tracking which routers are members of which VLANs and which router interfaces are in which VLAN. MVRP removes routers and interfaces from the VLAN information when they become unavailable. MVRP improves the convergence time of GARP VLAN Registration Protocol (GVRP). Defined by 802.1ak.

N

name resolution. The process of translating an IP address to a name that is easily remembered by a person. In a TCP/IP environment, a name such as www.ipinfusion.com is translated into its IP equivalent by the Domain Name Service (DNS).

neighbor. An adjacent system reachable by traversing a single subnetwork; an immediately adjacent device. Also called peer. See also adjacency.

Neighbor Discovery Protocol (NDP). An IPv6 protocol that nodes on the same link use to discover each other's presence, determine each other's Link Layer addresses, find routers, and maintain reachability information about the paths to active neighbors. NDP is defined in RFC 2461 and is equivalent to the Address Resolution Protocol (ARP) used with IPv4.

NETCONF (Network Configuration Protocol). A mechanism to install, manipulate, and delete the configuration of network devices. The operations, notifications, and the database contents supported by a particular NETCONF server are extensible, and defined with a modeling language called YANG. The database is used to store YANG data structures which represent the configuration of the device containing the NETCONF server. This configuration can be saved in non-volatile storage so the configuration can be restored upon reboot. Defined in RFC 6241.

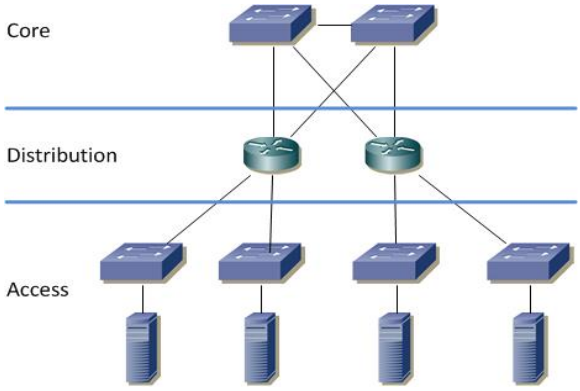
network. A group of computers and related devices connected by a communications channel capable of sharing resources among several users. A network consists of transmission media, devices such as routers or switches, and protocols that make message sequences meaningful.

A network can range from a peer-to-peer network connecting a small number of users in an office or department, to a Local Area Network (LAN) connecting many users, to a wide area network (WAN) connecting users on several networks spread over a wide geographic area.

network address translation (NAT). A method to use one set of IP addresses for an internal inetwork and a second set of addresses for the public Internet. This allows an organization to shield internal addresses from the public Internet. NAT is configured on the router at the border of an internal network and the Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the Internet and vice versa. Defined by RFC 1631.

network administrator. The person responsible for the day-to-day operation and management of a network.

network design model. A hierarchical model originally defined by Cisco that divides a network into three functional areas, or layers. This model optimizes network hardware and software to perform specific roles.



The roles that each layer performs are:

- The access layer provides local user access to the network
- The distribution layer connects network services to the access layer, and implements policies regarding security, traffic loading, and routing
- The core layer provides high-speed transport for the distribution layer

See also collapsed core.

Network Element (NE). Any device in a network such as a host, router, switch, or firewall that performs a service or function for the network.

Network Functions Virtualization (NFV). The ability to decouple network services from dedicated hardware devices to be hosted on a virtual machine (VM). Once the network services are under the control of a hypervisor, the services can be performed on standard x86 servers.

network layer. See Layer 3 (L3).

Network Layer Reachability Information (NLRI). Information exchanged between Border Gateway Protocol (BGP) routers in update messages. An NLRI contains a length and a prefix. The length is a network mask in Classless Interdomain Routing (CIDR) notation (such as /23) specifying the number of network bits, and the prefix is the network address for that subnet. NLRIs are unique to BGP version 4 and allow BGP to carry supernetting information, as well as perform aggregation. Examples of NLRIs are:

- /25, 204.149.16.128
- /8, 10

Only one NLRI is included in an update message, although there may be multiple AS-paths and AS-path attributes.

network segment. A portion of a computer network that is separated from the rest of the network by a device such as a router or switch. Each segment can contain one or more hosts.

Network Services Module (NSM). The base module in ZebOS-XP that communicates with every ZebOS-XP routing and switching process. The protocol components use APIs exposed by the NSM client, which act as conduits to transfer data between the protocol modules and NSM.

Network Time Protocol (NTP). A protocol used to synchronize the system clocks of hosts on a network to Universal Coordinated Time (UTC). A device can update its clock automatically by configuring itself as an NTP client. Using NTP enables the device to record accurate times of events. Defined by RFC 5905.

Neutron. The networking component of OpenStack that provides “networking as a service” between virtual NICs managed by other OpenStack services.

Neutron provides a “plug-in” mechanism that lets network operators enable different technologies. It also lets tenants create multiple private networks and control their IP addressing. Organizations have control over security and compliance policies, Quality of Service (QoS), monitoring and troubleshooting, as well as the ability to deploy network services, such as a firewall, intrusion detection, and Virtual Private Network (VPN) instances.

next hop. The next device to which a protocol data unit (PDU) is sent on its way to its destination.

Next Hop Label Forwarding Entry (NHLFE). An Multi-Protocol Label Switching (MPLS) entry containing next hop information (interface and next hop address) and label manipulation instructions; it can also include label encoding, L2 encapsulation information, and other information to process packets in the associated stream.

node. An addressable device such as a host, router, or switch, attached to a network, that transmits and receives data.

north/south. The flow of traffic traversing between users and a data center (spanning-tree). Contrast with east/west.

northbound. An interface that allows a network component to communicate with a higher-level component. A northbound interface hides complex details of operations. Northbound flow can be thought of as going upward. In architectural diagrams, northbound interfaces are drawn at the top of the component. See also southbound.

Not-So-Stubby-Area (NSSA). An extension of a Open Shortest Path First (OSPF) stub area. OSPF uses an NSSA as a transit to send external routes to other areas or to domains that are not part of the OSPF autonomous system. OSPF does not flood external routes from other areas into an NSSA, but does translate and flood route information from the NSSA into other areas such as the backbone. Defined by RFC 1587.

O

Open Network Foundation (ONF). A non-profit organization responsible for the development and standardization of a software architecture that supports Software-Defined Networking (SDN). ONF is also responsible for the commercialization and promotion of SDN as a concept and its underlying technologies. For more, see: https://www.opennetworking.org/.

Open Shortest Path First (OSPF). An Interior Gateway Protocol (IGP) based on link-state routing. OSPF is widely deployed in large networks because of its efficient use of network bandwidth and its rapid convergence after changes in topology. Defined in RFCs 2328 and RFC 5340.

OSPF advertises the states of local network links within an autonomous system (AS) and makes routing decisions based on the shortest path first (SPF) algorithm. Each OSPF router maintains an identical database describing the autonomous system's topology. From this database, a Routing Information Base (RIB) is calculated by constructing a shortest path tree (SPT).

OSPF features include least-cost routing, multipath routing, and load balancing. OSPF includes explicit support for Classless Interdomain Routing (CIDR) and the tagging of externally derived routing information.

OSPF version 2 supports IPv4 and OSPF version 3 supports IPv6.

OSPF divides an autonomous system into contiguous groups of networks called areas.

- In a standard area, intra-area routes, inter-area routes, and external routes (learned from other routing protocols such as RIP and BGP) are distributed. Inter-area routes and external routes are distributed as summary addresses.
- A backbone area is essentially a standard area which has been designated as the central point to which all other areas connect. A backbone area combines a set of independent areas into an AS and acts as a hub for inter-area transit traffic and routing information distribution. Each non-backbone area is directly connected to the backbone area.
- OSPF uses stub area instances and Not-So-Stubby-Area (NSSA) instances to limit distribution of inter-area routes and external routes.

See also area border router (ABR), autonomous system border router (ASBR).

Open Systems Interconnection (OSI) Reference Model. A conceptual model defined by the International Organization for Standardization (ISO) that organizes the computer-to-computer communications process into seven layers. Each layer provides services to the layer above and receives services from the layer below. Such a set of layers is called a protocol stack.

Layers seven through five manage end-to-end communications between the message source and destination, while layers one through four manage network access:

- Layer 4 (L4) ensures the end-to-end delivery from a source to a destination
- Layer 3 (L3) routes packets of data from source to destination across a network
- Layer 2 (L2) reliably transports data across the physical link between two directly connected nodes
- Layer 1 (L1) conveys the bit stream at the electrical and mechanical level

The OSI Reference Model is often compared to the more descriptive (versus prescriptive) Transmission Control Protocol/Internet Protocol (TCP/IP) model.

Open vSwitch (OVS). A software switch used in virtualized server environments that forwards traffic between different virtual machine (VM) instances on the same physical host and between VMs and the physical network. OVS enables network automation through programmatic extension, while still supporting standard management interfaces and protocols. For more, see http://openvswitch.org/.

OpenFlow. An open standard for forwarding plane operations that enables researchers to run experimental protocols. OpenFlow is developed, specified, and sponsored by the Open Network Foundation (ONF). OpenFlow provides a protocol that enables a controller to dynamically program internal flow-tables in devices. Network vendors have added OpenFlow features to routers and switches.

OpenStack. A cloud operating system that controls pools of compute, storage, and networking resources in a data center which users manage through a Web-based dashboard, command-line tools, or a RESTful API. See also Neutron.

Operation, Administration, and Maintenance (OAM). A set of Ethernet specifications that provide connectivity monitoring, fault detection and notification, fault verification, fault isolation, loopback, and remote defect identification. The primary specifications are 802.3ah link-fault management (LFM) and 802.1ag Connectivity Fault Management (CFM).

P

packet. A protocol data unit (PDU) at Layer 3 (L3) of the Open Systems Interconnection (OSI) Reference Model. A packet contains source and destination addresses, user data, and control information such as the length of the packet,

the header checksum, and flags indicating whether the packet has been fragmented. The user data in a packet is often referred to as the payload. The actual format of a packet depends on the protocol that creates the packet.

A packet sent through a connectionless protocol such as User Datagram Protocol (UDP) is sometimes called a datagram.

See also frame, packet switching.

packet switching. A data-transmission method that transmits information over one of several routes. Information is sent to the destination through the best route, determined by a routing algorithm.

A packet switched network breaks information to be transmitted into discrete packets. Related packets might not all follow the same path to their destination. Packet sequence numbers are used to reassemble the original message at the destination.

A packet-switched network is connectionless because each packet contains its destination address and does not require a dedicated path to reach that destination. Multiple users may transmit packets over the same connection at the same time, independent of one another.

The Internet is an example of a packet-switched network.

Contrast with circuit switching.

paravirtualized. A software component that is aware that it is running in a virtual machine (VM). For example, a paravirtualized virtual device driver runs in a VM that communicates with the underlying host OS. Typically, a paravirtualized driver is optimized to share queues, buffers, or other data items with the underlying host OS to improve throughput and reduce latency.

path computation element (PCE). An entity (component, application, or server) that can compute a network path or route based on a network graph and constraints (see RFC 4655).

path-vector routing. A routing technique that advertises a network as a destination address and a complete path to reach that destination. Each entry in the Routing Information Base (RIB) contains the destination network, the next router, and the path to reach the destination.

A path vector protocol guarantees loop-free paths by recording each hop the routing advertisement traverses through the network. A node can easily detect a loop by looking for its own node identifier in the path.

This technique is sometimes used in Bellman-Ford algorithm to avoid count-to-infinity problems.

Border Gateway Protocol (BGP) is an example of a prefix-based path-vector protocol where the Routing Information Base (RIB) maintains the autonomous systems to traverse to reach a destination.

peer. Immediately adjacent device with which a protocol relationship has been established. Also called neighbor.

penultimate hop popping (PHP). A technique where the outermost label of an Multi-Protocol Label Switching (MPLS) packet is removed by a label switch router (LSR) before the packet is passed to an adjacent label edge router (LER).

physical layer. See Layer 1 (L1).

ping (packet internet groper). A command used to test network connectivity by transmitting an Internet Control Message Protocol (ICMP) diagnostic packet to a specific node on the network, forcing the node to acknowledge that the packet reached the correct destination. If the node responds, the link is operating; if not, something is wrong.

The word ping is often used as a verb, as in “ping that workstation to see if it is alive.”

policing. Applying rate limits on bandwidth and burst size for traffic for a particular interface.

policy-based routing (PBR). Classifying packets to determine their forwarding path within a device. PBR is used to redirect traffic for analysis. Also called filter-based forwarding (FBF).

port. The point at which a communications circuit terminates on a network. A port can be logical, physical or both. Examples include:

- The physical interface between a device and a communications circuit, usually identified by a number or name.
- The logical interface between a TCP/IP applications and a communications facility which use well-known port numbers such as FTP: 20, HTTP: 80, and NFS: 2049.
- The logical interface between a process and a communications facility that allows more than one logical port to be associated with one physical port. For example, Ethernet uses multiple MAC addresses to distinguish between separate logical channels connecting two ports on the same physical transport network interface.

Also called interface.

port authentication. A mechanism for port-based user authentication and network access control for LAN devices. Defined by IEEE 802.1X.

Precision Time Protocol (PTP). A protocol that synchronizes clocks throughout a computer network. On a LAN, PTP achieves clock accuracy in the sub-microsecond range, making it suitable for measurement and control systems. The time synchronization is achieved through packets that are transmitted and received in a session between a master clock and a slave clock. Defined by IEEE 1588v2.

Priority-based Flow Control (PFC). A flow control mechanism that can be set independently for each frame priority on full-duplex links. Defined by IEEE 802.1Qbb.

private VLAN (PVLAN). A switch with ports that cannot communicate with each other, but can access other networks. A PVLAN has at least one private port and a trunk port. All traffic received on a private port is forwarded out the trunk port. All traffic received on a trunk port is handled as normal switch traffic. No traffic communication occurs between the private ports.

protocol. A set of rules that end points in a network connection must follow when they communicate. A protocol includes data representation, data item ordering, message formats, message and response sequencing rules, block data transmission conventions, and timing requirements.

The Open Systems Interconnection (OSI) Reference Model and Transmission Control Protocol/Internet Protocol (TCP/IP) are both used as a model for many protocols. There are one or more protocols at each layer in the models that both ends of the connection must recognize and observe.

protocol data unit (PDU). A unit of data transmitted as a composite by a protocol.

In the Open Systems Interconnection (OSI) Reference Model, the actual name used for a PDU depends on the layer:

- Layer 4 (L4): segment
- Layer 3 (L3): packet
- Layer 2 (L2): frame
- Layer 1 (L1): stream, symbol stream, or bit stream

See also bridge protocol data unit (BPDU). Sometimes called datagram.

Protocol Independent Multicast (PIM). A method to determine the best paths for distributing a multicast transmission. PIM uses unicast routing tables (such as those used by Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP)) and static routes to perform multicasting. Each host must be registered using IGMP to receive the transmission.

PIM has these variations:

- PIM dense mode (PIM-DM: RFC 3973) uses a push model. PIM-DM initially floods multicast traffic throughout the network. Routers that have no downstream neighbors prune back the unwanted traffic. This process repeats periodically.
- PIM sparse mode (PIM-SM: RFC 4601) uses a pull model. PIM-SM uses a shortest path tree (SPT) where sources forward multicast packets to a designated router which unicasts the packets to an assigned rendezvous point router, which then forwards the packets to members of multicast groups.
- PIM source-specific multicast (PIM-SSM: RFC 3569) uses PIM-SM functionality to create a SPT between the client and the source without using a rendezvous point.
- Bidirectional PIM (Bidir-PIM: RFC 5015) uses PIM-SM functionality to route traffic only along a bidirectional SPT that is rooted at the rendezvous point for a group.

protocol stack. The layers of software used in network communications.

Provider Backbone Bridge-Traffic Engineering (PBB-TE) . An extension to Provider Backbone Bridging (PBB) that removes features such as flooding, dynamically created forwarding tables, and spanning tree protocols. PBB-TE also covers Connectivity Fault Management (CFM) and Ethernet Linear Protection Switching (ELPS).

In PBB-TE, a network administrator configures the forwarding tables in the backbone switches with static routes to ensure that frames take predetermined paths within the network. Frames with destination MAC addresses not in a forwarding table are dropped. Broadcast frames are not supported and are also dropped by backbone switches.

Defined in IEEE 802.1Qay.

Provider Backbone Bridging (PBB). A technique to create Ethernet backbones for service access networks. Defined in IEEE 802.1ah, PBB extends Provider Bridging (PB) defined in 802.1ad in these ways:

- The 802.1ah header adds an I-SID (Service Instance Identifier) which is a label that maps to a customer VLAN identifier. An I-SID virtualizes VLANs across a network. VLANs are mapped into I-SIDs by configuring only the edge of the network at a backbone edge bridge (BEB). This makes the maximum number of service instances 16 million.
- The 802.1ah header encapsulates backbone source and destination MAC addresses (B-MAC) along with the customer source and destination MAC addresses (C-MAC). The B-MAC contains MAC addresses of the service provider's PBB edge switches. The 802.1ah format is sometimes called “MAC-in-MAC” because of this MAC address encapsulation. The encapsulation of customer MAC addresses in backbone MAC addresses means that the backbone does not need to learn customer MAC addresses. Customer MAC addresses are learned at BEB ports only.

Provider Bridging (PB). A technique that enables a service provider to use the architecture and protocols of 802.Q to offer the equivalent of separate LANs, bridged LANs, or VLANs to multiple customers. Provider bridging requires no active cooperation between customers and requires minimal cooperation between an individual customer and the service provider.

When VLANs were originally defined in 802.1Q, the number of unique VLAN identifiers was limited to 4096. In large provider networks, each subscriber needs a separate address, so this limit could prevent a provider from having more than 4096 subscribers.

To overcome this limit, 802.1ad inserts an additional VLAN tag into a single 802.1Q Ethernet frame. Frames passing through the provider network are doubly tagged with:

- customer VLAN (C-VLAN) tag which identifies the customer network VLAN
- service VLAN (S-VLAN) tag which identifies the service provider network VLAN

With two VLAN identifiers in combination for each provider-customer pair, it is possible to define up to 16,777,216 VLANs.

The frame format for 802.1ad is also called Q-in-Q, double tagged, stacked VLANs, or VLAN stacking.

provider edge (PE). A device at the edge of an enterprise or service provider core network. A PE offers an initial, first level of network traffic aggregation for many customer edge (CE) devices.

pseudowire (PW). An emulation of a point-to-point connection over a packet-switching network. A pseudowire is a way to transport legacy services such as TDM over a packet-switched network:

- Structure-aware TDM circuit emulation service over packet-switched network (CESoPSN)
- Structure-agnostic TDM over packet (SAToP)

A pseudowire that both originates and terminates on the edge of a single packet-switched network (autonomous system or carrier network) is called a single-segment pseudowire (SS-PW). A pseudowire that extends through multiple autonomous systems or carrier networks is called a multi-segment pseudowire (MS-PW).

Q

Q-in-Q. See Provider Bridging (PB).

QEMU (Quick EMUlator). A hosted hypervisor that performs hardware virtualization. QEMU emulates CPUs through dynamic binary translation and provides a set of device models enabling it to run a variety of unmodified guest operating systems. QEMU also can be used together with KVM (Kernel-based Virtual Machine) to run virtual machines at near-native speed (requiring hardware virtualization extensions on x86 machines). QEMU can also be used purely for CPU emulation for user-level processes, allowing applications compiled for one architecture to be run on another.

Quality of Service (QoS). The ability to *guarantee* the delivery, control the bandwidth, set priorities for specific network traffic, and provide an appropriate level of security. QoS provides a level of predictability and control beyond the best effort delivery that a device provides by default.

See also Class of Service (CoS).

Quantized Congestion Notification (QCN). An end-to-end congestion management scheme for protocols capable of transmission rate limiting. Defined by IEEE 802.1Qau.

R

radio access network (RAN). The air interface and base station technology in a cellular network. In addition to the RAN, the entire cellular system includes the core network, which provides the backbone and services, as well as the cellphones.

Rapid Per-VLAN Spanning Tree Plus (RPVST+). A version of Cisco Per VLAN Spanning Tree Plus (PVST+) that uses the Rapid Spanning Tree Protocol (RSTP) state machine. PVST+ runs a spanning tree instance for each VLAN in the network. PVST+ is not scalable when there are many VLANs in a network. A compromise between RSTP and R-PVST+ is Multiple Spanning Tree Protocol (MSTP) which runs multiple instances of spanning tree that are independent of VLANs. MSTP maps a set of VLANs to each spanning tree instance.

Rapid Spanning Tree Protocol (RSTP). An enhancement to the Spanning Tree Protocol (STP) that re-configures quickly after a topology change. RSTP can verify if a port can change to a forwarding state safely without waiting for timers to start convergence. RSTP is not aware of VLANs and blocks ports at the physical level. Defined by IEEE 802.1D. See also Multiple Spanning Tree Protocol (MSTP).

Remote Authentication Dial In User Service (RADIUS). An authentication and accounting protocol to authenticate users and authorize their access to the requested system or service.

Defined in RFCs 2058, 2059, and 2865. See also authentication, authorization, and accounting (AAA), Lightweight Directory Access Protocol (LDAP), Terminal Access Controller Access Control System Plus (TACACS+).

remote monitoring (RMON). A Management Information Base (MIB) specification that defines functions for remotely monitoring networked devices. The RMON specification provides many problem detection and reporting capabilities. Defined by RFC 2819.

Request for Comments (RFC). Proposals and standards that define protocols for communications over the Internet. RFCs are developed and published by the Internet Engineering Task Force (IETF).

Resource Reservation Protocol (RSVP). A signalling protocol for reserving resources across a network. RSVP is rarely used by itself, but Resource Reservation Protocol—Traffic Engineering (RSVP-TE) is widely used.

Resource Reservation Protocol—Traffic Engineering (RSVP-TE). RSVP with traffic engineering extensions, as defined by RFC 5101, that allows RSVP to establish label-switched path (LSP) instances in Multi-Protocol Label Switching (MPLS) networks, using Constrained Shortest Path First (CSPF), taking into consideration constraints such as available bandwidth and explicit hops. The LSPs might not agree with the route suggested by the Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS).

reverse path forwarding (RPF). An algorithm that checks the unicast Routing Information Base (RIB) to determine whether there is a shortest path back to the source address of an incoming multicast packet. Unicast RPF helps determine the source of denial-of-service attacks and rejects packets from unexpected source addresses.

Rivest-Shamir-Adleman (RSA). A public key, or asymmetric, encryption scheme. The theoretical background to RSA is that it is difficult to find the factors of a very large number that is the product of two prime numbers. RSA is considered very secure provided a sufficiently long key is used.

route. The path from source to destination through a network.

route flap damping. Method for minimizing instability caused by route flapping. The router stores a penalty value for each route. Each time the route flaps, the router increases this value. If the penalty for a route reaches a configured suppress value, the router does not include the route as a forwarding entry and does not advertise the route to peers.

route redistribution. One protocol learning routes from another protocol running on the same device. Also called redistribution or route leakage.

route reflection. A method of allowing iBGP routers to accept and propagate iBGP routes to their clients.

To avoid routing loops, Border Gateway Protocol (BGP) does not advertise routes learned from an internal BGP peer to other internal BGP peers. Instead, BGP requires that all internal peers be fully meshed so that any route advertised by one router is advertised to all peers within the autonomous system (AS). As a network grows, the full mesh requirement becomes difficult to manage. To handle scaling problems, BGP uses route reflection and BGP confederations.

Route reflection allows you to designate one or more routers as route reflectors. BGP relaxes the re-advertising restriction on route reflectors, allowing them to accept and propagate iBGP routes to their clients.

route summarization. Consolidating multiple routes into a single route advertisement, in contrast to flat routing where a Routing Information Base (RIB) contains a unique entry for each route.

Classless Interdomain Routing (CIDR) is used to implement route summarization. All IP addresses in the route advertisement must have identical high-order bits.

Also called route aggregation. See also subnet mask.

router. A Layer 3 (L3) device that makes decisions about the paths over which network traffic will flow. Routers use dynamic routing protocols to learn about the network and to find the best route to forward packets toward their final destination:

1. Find a matching destination address in the Routing Information Base (RIB)
2. Find the MAC address for the packet from the Address Resolution Protocol (ARP) cache
3. Write the new MAC address in the IP packet
4. Send the packet on the port associated with the MAC address

routing. The process of finding a path to a destination to use to transmit a protocol data unit (PDU) over a network. Routing is usually controlled by a Routing Information Base (RIB) which defines where a PDU should go. Each router only needs to know where a PDU should be sent on its next hop, and does not know nor care what happens afterward; the next hop plus one is the responsibility of the next router, and so on through the network until a PDU reaches its destination.

Routing Information Base (RIB). A data structure in a device that lists the routes to destinations and metrics (distances) associated with those routes. A RIB contains information about the topology of the network immediately around it. Maintaining a RIB by discovering network topology is the primary purpose of dynamic routing protocols such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP), and Open Shortest Path First (OSPF). Network administrators can also add fixed routes to the RIB for static routing.

Also called a routing table. Contrast with Forwarding Information Base (FIB).

Routing Information Protocol (RIP). An Interior Gateway Protocol (IGP) that implements a distributed variant of the Bellman-Ford algorithm to provide distance-vector routing capabilities. RIP uses the hop count of a destination to detect the best path to route packets, but limits the maximum number of hops to 15 to prevent routing loops. RIP implements split horizon techniques. Defined in RFC 1058.

RIP is easy to configure and has low processing requirements. However, the hop count limit restricts the size of the network that RIP can support. Also, RIP can be slow to converge.

RIPv2 defined in RFC 2453 also supports subnet information, allowing Classless Interdomain Routing (CIDR).

RIPng (next generation), an extension of RIPv2 defined in RFC 2080, supports IPv6.

routing protocol. A set of processes, algorithms, and messages that are used to exchange routing information and populate the local Routing Information Base (RIB) with the best path between a source and destination.

The term “routing protocol” usually implies dynamic routing, where a device reports changes and shares information with other devices in the network. Each router starts with knowledge of only the devices to which it is directly attached. The routing protocol shares this information first with its immediate neighbors, and then throughout the network. This way, routers learn the topology of the network.

A primary benefit of dynamic routing protocols over static routing is that routers exchange information when there is a topology change. This exchange allows routers to automatically learn about new devices and networks and also to find alternate paths when there is a link failure in the current network.

Table 3-2 summarizes the characteristics of the dynamic routing protocols supported by ZebOS-XP:

Table 3-2: Dynamic routing protocols

	Border Gateway Protocol (BGP)	Routing Information Protocol (RIP)	Open Shortest Path First (OSPF)	Intermediate System to Intermediate System (IS-IS)
Algorithm	path-vector routing	distance-vector routing	link-state routing	link-state routing
Type	Exterior Gateway Protocol (EGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)	Interior Gateway Protocol (IGP)
Classless Interdomain Routing (CIDR)	Yes	RIP v1: No RIP v2: Yes	Yes	Yes
Scalable	Yes	No	Yes	Yes
Speed of convergence	Moderate	Slow	Fast	Fast
Resource Use	High	Low	High	High
Configuration ease	Complex	Simple	Complex	Complex

routing table. See Routing Information Base (RIB).

S

S-TAG. See service VLAN (S-VLAN).

(S,G). A notation used in multicast that enumerates a shortest path tree (SPT) where:

- S is the IP address of the source
- G is the multicast group address that identifies the receivers

If the IP address of the source is 192.1.1.1, and the IP address of the multicast group is 224.1.1.1, the source group is written as (192.1.1.1, 224.1.1.1).

Secure Shell (SSH). A protocol that allows the opening of a secure, encrypted channel between two computers with secure authentication. SSH is most often used to provide a secure shell to log in to a remote machine, but also supports file transfers, TCP, and other functions.

segment routing. A form of source routing where nodes and links are represented as segments. The path that a particular protocol data unit (PDU) needs to traverse is represented by one or more segments.

server. A system entity that provides a service to other entities called clients.

service VLAN (S-VLAN). In a Provider Bridging (PB) frame, a tag that identifies the service provider network VLAN. See also customer VLAN (C-VLAN). Also called an S-TAG or S-VID tag.

Shortest Path Bridging (SPB). A control plane protocol that combines an Ethernet data path with an Intermediate System to Intermediate System (IS-IS) link state protocol running between switches. SPB does not depend on spanning tree protocols to provide a loop-free topology, but instead uses IS-IS link-state packets to discover and advertise the network topology and compute the shortest path tree (SPT) instances from all bridges in the SPB area. SPB only requires provisioning at the edge of the network. Defined by IEEE 802.1aq, with RFC 6329 describing the IS-IS extensions to support SPB.

There are two types of SPB depending on the type of Ethernet data path:

- Shortest Path Bridging - VID (SPBV) uses a Provider Bridging (PB) (802.1ad) data path
- Shortest Path Bridging - MAC (SPBM) uses a Provider Backbone Bridging (PBB) (802.1ah) data path

shortest path first (SPF). Algorithm used by Intermediate System to Intermediate System (IS-IS) and Open Shortest Path First (OSPF) to make routing decisions based on the state of network links. Also called the Dijkstra algorithm.

shortest path tree (SPT). A Routing Information Base (RIB) formed by using the shortest path first (SPF) algorithm.

shortest-path routing. A routing algorithm in which paths to all network destinations are calculated. The shortest path is then determined by a cost assigned to each link.

signalling. The ability to transfer information within a network or between different networks.

Simple Network Management Protocol (SNMP). A standardized framework for monitoring and managing devices in a network. The SNMP framework consists of three parts:

- SNMP manager: The system used to control and monitor the activities of network devices.
- SNMP agent: The component within a managed device that maintains the data for the device and reports the data SNMP managers.
- Management Information Base (MIB): How SNMP exposes data as variables which describe the system configuration. These variables can be queried (and sometimes set) by SNMP managers.

SNMP uses User Datagram Protocol (UDP) to send and receive messages on the network.

Single Root I/O Virtualization (SR-IOV). A specification that allows a single Peripheral Component Interconnect Express (PCIe) physical device under a single root port to appear to be multiple separate physical devices to the hypervisor or the guest operating system.

SR-IOV uses physical functions (PFs) and virtual functions (VFs) to manage global functions for the SR-IOV devices:

- PFs are used to configure and manage the SR-IOV functionality
- VFs are lightweight and contain all the resources necessary for data movement but have a minimal set of configuration resources

SR-IOV enables network traffic to bypass the software switch layer of a virtualization stack. The I/O overhead in the software emulation layer is nearly the same as in nonvirtualized environments.

Software-Defined Networking (SDN). An approach to designing, building, and operating networks that decouples the control plane from the data plane. The control plane is centralized in the form of a controller system. Communication between the controller system and the network device uses a standard protocol such as OpenFlow or other agents. The controller system can consist of multiple, domain specific, clustered controllers. An SDN architecture usually includes APIs that developers use to control the underlying network. These APIs can be standards-based, or they can be vendor-specific.

source routing. A technique where the sender of a protocol data unit (PDU) can partially or completely specify the route that the PDU should take through the network. See also segment routing.

southbound. An interface that allows a network component to communicate with a lower-level component. A southbound interface breaks down the concepts into smaller technical details that are specifically geared toward the lower-layer component within the architecture. Southbound flow can be thought of as going downward. In architectural diagrams, southbound interfaces are drawn at the bottom of the component. See also northbound.

spanning tree algorithm. A technique that finds the best path between segments of a multilooped, mesh network. If multiple paths exist in the network, the spanning tree algorithm finds the most efficient path and limits the link between the two networks to this single active path. If this path fails because of a cable failure or other problem, the algorithm reconfigures the network to use another path.

From the point of view of an individual switch, a spanning tree has a root node and one path that connects all the other switches.

Spanning Tree Protocol (STP). A protocol that creates spanning trees within mesh networks of connected devices, disabling any links that are not a part of the tree and leaving a single active connection between any two unique network nodes. Defined by 802.1D.

STP devices exchange bridge protocol data unit (BPDU) messages. The spanning tree algorithm calculates the best path and prevents multiple paths between network segments. STP elects a root bridge, finds paths and determines the least cost path to the root bridge, then disables all other paths.

Network managers can set up redundant links as backups in case active links fails. Automatic backup takes place without the pitfalls of bridge loops or the need to manually enable or disable backup links.

See also Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP).

split horizon. A technique where routes learned from an interface are not advertised on that same interface, preventing the router from seeing its own route updates.

In split horizon with poison reverse, routes learned from an interface are set as unreachable and advertised on that same interface which also prevents the router from seeing its own route updates.

stacked VLAN. See Provider Bridging (PB).

static address. An address permanently assigned to a device. Contrast with a dynamic address.

static routing. A method where a network administrator programs connecting paths between networks into a router. If a connection fails, the administrator must reprogram the router to use a new path. Static routes have precedence over routes chosen by dynamic routing protocols.

stub area. A type of Open Shortest Path First (OSPF) area where external routes are distributed as a single default route (address 0.0.0.0). Inter-area routes are distributed in a stub area as summary addresses.

In a *totally stubby area*, a single default route is distributed for all external *and* inter-area routes. Addresses from both other areas and external networks are distributed as the default route (address 0.0.0.0).

See also Not-So-Stubby-Area (NSSA).

subnet mask. A bit pattern that shows how an Internet address is divided into network, subnetwork, and host parts. The mask has ones in the bit positions to be used for the network and subnet parts, and zeros for the host part. The mask should contain at least the standard network portion, and the subnet field should be contiguous with the network portion.

This is an example is this IPv4 address and subnet mask:

192.168.100.12 with subnet mask of 255.255.255.0

The first 24 bits of the address is the network address (192.168.100.0) and the last 8 bits are the hosts (12). The entire subnet spans the address range 192.168.100.0 to 192.168.100.255.

The addresses on a given subnet are always contiguous and can all be derived from the network address. Bit masks are always with respect to binary digits, so the number of IP addresses on a given subnet is always some power of two.

A mask gives the first address in the block (the network address) when ANDed with an address in the block.

Classless Interdomain Routing (CIDR) represents the equivalent of a subnet mask by adding a prefix length to an IP address that is the number of bits in the network portion. For example, the subnet mask above can be written as:

192.168.100.12/24

where 192.168.100.12 is the IP address and /24 is the number of bits in the subnet mask.

A subnet mask represents the same information as a prefix length, but predates the use of CIDR.

Also called address mask, network mask.

subnetwork. A group of related IP addresses that all begin with the same network portion and end with a unique portion identifying the host within the subnet.

Also called subnet. See also subnet mask.

subsequent address family identifier (SAFI). A qualification such as unicast, multicast, or MPLS that further identifies an address family.

supernetting. The process of taking several discrete network addresses and advertising them as one route. For example, if an organization is using 192.10.1.0/24 to 192.10.254.0/24, instead of advertising 254 separate networks, the organization can advertise only the single route 192.10.0.0/16.

switch. A Layer 2 (L2) device that forwards frames based on a destination MAC address. A switch finds a destination address in its filtering database and transmits the frame on the port associated with the destination address. The filtering database is populated through a self-learning process, where each incoming frame is used to update the entries in the filtering database.

A switch that is VLAN-aware can also forward frames based on VLAN identifiers. A network administrator can configure this mapping manually or a switch can dynamically learn mappings via GARP VLAN Registration Protocol (GVRP).

Basic switch behavior is defined in IEEE 802.1D and 802.1Q.

See also bridge. Contrast with router.

Synchronous Ethernet (SyncE). SONET/SDH/PDH-based synchronization that is used to synchronize and send frequency information to devices on an Ethernet network. Synchronous Ethernet provides only frequency synchronization, not time or phase synchronization.

T

telnet. A client/server protocol that establishes a session between a user terminal and a remote host:

- The telnet client software takes input from the user and sends it to the server's operating system
- The telnet server takes output from the host and sends it to the client to display to the user

While telnet is most often used to implement remote login capability, the protocol is general enough to allow it to be used for a variety of purposes.

Terminal Access Controller Access Control System Plus (TACACS+). An authentication method that provides access control for networked devices using one or more centralized servers. TACACS+ provides separate

authentication, authorization, and accounting (AAA) services. (Usually pronounced like tack-axe.)

See also Lightweight Directory Access Protocol (LDAP), Remote Authentication Dial In User Service (RADIUS).

throughput. Average rate of successful delivery of data packets over a communication link. Throughput is measured in bits per second, data packets per second, or sometimes data packets per time slot. See also line rate, latency, wire speed.

time to live (TTL). A limit on how long a piece of information can exist before it should be discarded. TTL is a field in an IP header that is (usually) decremented by 1 for each hop through which the packet passes. If the field reaches zero, the packet is discarded, and a corresponding error message is sent to the source of the packet.

Top-of-Rack (ToR) switch. In a data center, an access layer switch that connects to servers installed in the same rack. A ToR switch is usually low profile (one or two rack units in height) with a low port count (typically 48 ports). All cabling for servers stays within the rack as relatively short cables from the servers to the switch. The switch connects the rack to the data center network with one fiber uplink to a distribution layer switch. There is no need to run cabling between racks and each rack can be managed as a modular unit.

A ToR switch extends the Layer 2 (L2) topology from the aggregation switch to each individual rack resulting in a larger Layer 2 footprint.

See also end-of-row switch.

topology. The physical or logical layout of a network.

topology change notification (TCN). In Spanning Tree Protocol (STP), a bridge protocol data unit (BPDU) that a switch sends to signal a topology change.

traffic engineering (TE). The ability to control the path taken through a network based on a set of traffic parameters. Traffic engineering optimizes the performance of networks and their resources by balancing traffic load across links, routers, and switches in the network. See also Resource Reservation Protocol—Traffic Engineering (RSVP-TE).

Transmission Control Protocol (TCP). A Layer 4 (L4) protocol that works above Internet Protocol (IP) and provides reliable data delivery over connection-oriented links.

TCP splits the stream of data into packets with a sequence number, and sends the packets over an IP-based network. At the destination, TCP acknowledges packets that have been received (so that missing packets can be resent) and reassembles received packets in the correct order to provide an in-order data stream to the remote application. If TCP detects a missing, corrupted, or out of order packet, it requests it be resent from the source.

See also Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP).

Transmission Control Protocol/Internet Protocol (TCP/IP). A family of Internet protocols that describe how data should be formatted, addressed, transmitted, routed, and received to enable computers to communicate over a network.

The Open Systems Interconnection (OSI) Reference Model is a more prescriptive (versus descriptive) approach to network design. TCP/IP does not map cleanly to the OSI model because it was developed before the OSI model and was designed to solve a specific set of problems, not to be a general description for all network communications.

TCP/IP is a widely published open standard and is supported by many vendors and is available on many different computers running many different operating systems. TCP/IP is separated from the network hardware and will run over Ethernet and other connections.

TCP/ IP also refers to the specific functionality at layers 4 and 3:

- Transmission Control Protocol (TCP) at Layer 4 (L4) splits a message into packets that are transmitted over the Internet and reassembles the packets into the original message at the destination
- Internet Protocol (IP) at Layer 3 (L3) addresses and routes each packet so that it gets to its destination

TRansparent Interconnection of Lots of Links (TRILL). Layer 2 (L2) bridging using Intermediate System to Intermediate System (IS-IS) link-state routing. TRILL encapsulates native frames in a transport header that contains a hop count, routes the encapsulated frames using IS-IS, and decapsulates the native frame before delivery.

Spanning tree protocols restrict all traffic to a loop-free tree and in doing so creates blocking conditions that require the over provisioning of links. With TRILL, you can create a fully meshed network where all links are available on all paths, eliminating the need to over-provision links and improving the utilization of data center networking equipment.

transport layer. See Layer 4 (L4).

tunneling. A method of transporting data in one protocol by encapsulating it in another protocol. Tunneling is used for reasons of incompatibility, implementation simplification, or security. For example, a tunnel lets a remote VPN client have encrypted access to a private network.

type of service (ToS). A field in the IPv4 header used to differentiate packet flows. See also Differentiated Services (DiffServ).

type-length-value (TLV). A data structure used to encode optional information in a data communications protocol:

- Type: the kind of field that this part of the message represents
- Length: the size of the value field, usually in bytes
- Value: a variable-sized set of bytes that contains the data of the message

U

unicast. The process of a single host sending messages to one destination.See also broadcast, multicast.

User Datagram Protocol (UDP). A connectionless transport layer protocol that exchanges datagrams without acknowledgments or guaranteed delivery and which requires other protocols to handle error processing and retransmission. Defined in RFC 768.

Multicast applications that deliver audio and video streams use UDP as their delivery mechanism because the acknowledgment and retransmission services offered by Transmission Control Protocol (TCP) are not needed and add too much overhead.

User-to-Network Interface (UNI). The physical interface/demarcation between a service provider and a subscriber, the service start or end point. There are two types of UNI:

- UNI-C: customer-side processes
- UNI-N: network-side processes

V

VirNOS. An IP Infusion product based on Network Functions Virtualization (NFV) that helps network operators deploy and manage networking services. Many core networking services, including switching, routing, load balancing and VPN can be performed by software either running directly on x86-64 servers or running as virtual machine (VM)

instances instead of requiring expensive networking equipment. Therefore, organizations are migrating networking functions to standard, high-volume server environments and replacing dedicated network hardware with virtualization software that runs on commodity servers. Carriers, service providers, enterprises and network equipment manufacturers can run VirNOS as-is, on top of a standard server platform. IP Infusion customers can integrate VirNOS into their software offering and thereby add services and features quickly.

Virtual Ethernet Bridge (VEB). A virtual switch implemented in a virtualized server environment. A VEB mimics a traditional external Layer 2 (L2) switch for connecting to a virtual machine (VM). VEBs can communicate between VMs on a single physical server, or they can connect VMs to the external network. The most common implementations of VEBs are software-based vSwitches built into hypervisors.

Virtual Local Area Network (VLAN). A logical group of network devices that appear to be on the same LAN, regardless of their physical location. VLANs enable multiple bridged LANs to transparently share the same physical network link while maintaining isolation between networks. Traffic between VLANs is restricted to devices that forward unicast, multicast, or broadcast traffic only on the LAN segments that serve the VLAN to which the traffic belongs.

VLANs make it easy to administer logical groups of hosts that can communicate as if they were on the same LAN.

Membership in a particular VLAN can be by port, MAC address, protocol, or subnet.

VLANs are configured as unique Layer 2 (L2) broadcast domains. VLANs allow network administrators to resegment their networks without physically rearranging the devices or network connections. VLANs span one or more ports on multiple devices and several VLANs can co-exist on a single physical switch. By default, each VLAN maintains its own filtering database containing MAC addresses learned from frames received on ports belonging to the VLAN.

IEEE 802.1Q provides for tagging Ethernet frames with VLAN identifiers. 802.1Q only supports up to 4094 VLANs, which is a scaling constraint for service providers.

virtual machine (VM). An operating system or application environment installed on emulated hardware and not physically installed on dedicated hardware. The virtual machine's guest operating system does not have to be modified to run in a virtualized environment. A VM behaves like a traditional, physical server and runs a traditional operating system such as Windows or Linux.

A hypervisor emulates the computer's CPU, memory, hard disk, network and other hardware resources completely, enabling virtual machines to share the resources. The hypervisor can emulate multiple virtual hardware platforms that are isolated from each other. For example, virtual machines can run Linux and Windows operating systems and share the same underlying physical host. An operating sysem is unaware that it is running in a VM.

See also paravirtualized, virtualization.

virtual port. A port on a vSwitch (Virtual Switch) where virtual Ethernet adapters or physical uplinks can be attached. During their creation, virtual switches are typically configured with a specific number of virtual ports.

virtual private LAN service (VPLS). Multipoint-to-multipoint Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone.

VPLS evolved as a logical extension of Virtual Private Wire Service (VPWS) based on RFC 4447.

VPLS can be defined as several instances of a virtual switch instance (VSI) that are interconnected to form a single logical bridge domain.

Virtual Private Network (VPN). A network service which uses encryption and tunneling to provide a subscriber with a secure private network that runs over the public network infrastructure.

Virtual Private Wire Service (VPWS). Point-to-point Layer 2 (L2) VPN service used to interconnect multiple Ethernet LANs across an Multi-Protocol Label Switching (MPLS) backbone. Also called Virtual Leased Line (VLL) or Ethernet over MPLS (EoMPLS).

virtual router (VR). A ZebOS-XP proprietary abstraction where multiple distinct logical routers exist within a single device. Each virtual router executes separate instances of the routing protocol and network management software. A virtual router provides support for multiple Routing Information Base (RIB) instances and multiple Forwarding Information Base (FIB) instances per physical router. Each VR might consist of an Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), or Routing Information Protocol (RIP) routing process, each with its own Routing Information Base (RIB) and Forwarding Information Base (FIB). Applications include segregating traffic dedicated to different customers, enterprise Virtual Private Network (VPN) users, or a specific traffic type such as streaming video.

Do not confuse a Virtual Router Redundancy Protocol (VRRP) virtual router with a ZebOS-XP virtual router. They are two different things.

Virtual Router Redundancy Protocol (VRRP). A protocol that uses a *virtual router*, an abstract representation of multiple routers (master and backup routers) that act as a group. VRRP advertises a virtual router as the default gateway instead of one physical router. Two or more physical routers are configured, with only one doing the actual routing at any given time. If the current physical router that is routing on behalf of the virtual router fails, the other physical router automatically takes over. Defined by RFC 5798.

Do not confuse a VRRP virtual router with a ZebOS-XP virtual router (VR). They are two different things.

Virtual Routing and Forwarding (VRF). A technology that allows multiple instances of a Routing Information Base (RIB) to co-exist within the same router at the same time. Multiple VRFs inside a virtual router (VR) logically subdivide the RIBs. Service providers can use VRF technology to create a separate Virtual Private Network (VPN) for each of their customers. Therefore, the technology is also called VPN routing and forwarding.

virtual switch instance (VSI). A mechanism for VLANs to pass packets to other VLANs without sending the packets through a router. With a VSI, the switch recognizes packet destinations that are local to the sending VLAN and bridges (switches) those packets. Only packets destined for another VLAN are routed.

A VSI is similar to the bridging defined in IEEE 802.1Q; a frame is switched, based on the destination MAC and membership in a Layer 2 (L2) VPN. A VSI floods unknown, broadcast, or multicast frames to all ports associated with the VSI.

virtualization. A technology that abstracts the physical characteristics of a machine, creating a logical version of it, including creating logical versions of entities such as operating systems and network resources. See also hypervisor, virtual machine (VM).

vNIC (Virtual Network Interface Card). Software that behaves like a Ethernet hardware adapter. It has a MAC address, and it sends and receives Ethernet frames.

VPN routing and forwarding. See Virtual Routing and Forwarding (VRF).

vSwitch (Virtual Switch). Software that behaves like a physical Ethernet switch. A vSwitch connects virtual machine (VM) instances in a virtual network at layer 2:

- Connects vNIC (Virtual Network Interface Card) instances from multiple VMs to virtual ports
- Connects physical network interface cards to virtual ports
- Uplinks to the physical network

A vSwitch maintains a MAC address table and routes traffic to specific ports, rather than repeating traffic on all ports. A vSwitch can include other features found in physical Ethernet switches, such as VLANs.

See also Open vSwitch (OVS).

W

weighted fair queuing (WFQ). Queue scheduling discipline where each queue has a weight and is assigned a different percentage of output port bandwidth. WFQ supports variable-length packets so that flows with larger packets are not allocated more bandwidth than flows with smaller packets.

WFQ classifies traffic as high- or low-bandwidth with low-bandwidth traffic getting priority and high-bandwidth traffic sharing what is left over. If traffic bursts ahead of the rate at which the interface can transmit, new high-bandwidth traffic is discarded after a congestive-messages threshold has been reached.

WFQ provides preferential treatment for higher priority traffic while preventing total starvation of lower priority traffic under sustained overload conditions.

weighted random early detection (WRED). Congestion avoidance mechanism which prevents an output queue from ever filling to capacity. WRED provides separate thresholds and weights for different IP precedences, allowing you to provide different qualities of service in regard to packet dropping for different traffic types. Standard traffic may be dropped more frequently than premium traffic during periods of congestion.

weighted round-robin queuing (WRR). Queue scheduling discipline that supports flows with significantly different bandwidth requirements. Each queue can be assigned a weight that is relative to other queues. WRR ensures that lower-priority queues are not denied access to buffer space and output port bandwidth. At least one packet is removed from each queue during each service round.

white box switch. In computer hardware, a white box is a server without a well-known brand name made from commonly available parts. White box switches are like white box servers, offering low cost without the brand name or tight integration of silicon and network software features.

Traditional black box switches are built with vertically integrated hardware and software. Some vendors use custom application-specific integrated circuit (ASIC) components to boost performance and add features, which adds to the cost. A white box switch decouples the software from the switching hardware. By decoupling software and hardware, customers have more flexibility and can potentially change software without changing hardware.

A white box switch runs a network operating system on generic x86 hardware with “merchant silicon” chipsets from manufacturers such as Broadcom, Centec, Intel, Marvell, and Mellanox. White box switches rely on an operating system such as Linux to integrate the Layer 2 (L2)/Layer 3 (L3) networking functions.

White box switches do not have the same complex features as black box switches because most interact with Software-Defined Networking (SDN) controllers to make forwarding and control plane decisions from a centralized point for all switches in the network. The SDN controller uses OpenFlow (or another southbound API) to program the forwarding table of the white box switches.

Some vendors sell a complete white box solution with the operating system already installed, while others supply just the “bare-metal” switch and you buy the operating system direct from the software vendor.

wide area network (WAN). A network that provides communication services to a geographic area larger than that served by a Local Area Network (LAN) and that may use or provide public communication facilities.

wire speed. The ability of a device to achieve throughput equal to the maximum throughput of a communication standard.

Y

YANG. A data modeling language that specifies the syntax and semantics for NETCONF (Network Configuration Protocol) operations, notification events, and database content. YANG tools can automate behavior within the NETCONF protocol for clients and servers.

YANG can model both configuration and state data of network elements. YANG structures the data definitions into tree structures and provides many modeling features, including an extensible type system, formal separation of state and configuration data and a variety of syntactic and semantic constraints. YANG data definitions provide a strong set of features for extensibility and reuse. Defined in RFC 6020.

Z

ZebHA. An IP Infusion product that ensures a pre-agreed level of operational performance by minimizing system downtime. A ZebHA system operates redundant nodes that can provide continued service when a node fails. High availability does not mean that components will never fail, but it ensures that the system is available when the user needs it even if components fail. ZebHA provides:

- Simplex-Active or Active-Standby (1+1) control plane redundancy
- Reliable handling of operational, application, system and component failures;
- Strict Service Level Agreements (SLA) requirements of network operator customers

ZebHA supports protocol modules in Layer 2 (L2) and Layer 3 (L3).

There are two types of protocol recovery after a redundancy switchover: stateful switchover (SSO) and graceful restart.

ZebIC. An IP Infusion product that enables network equipment manufacturers to develop networking solutions based on leading silicon platforms. ZebIC allows manufacturers to deliver networking products built around this switching platform.

ZebIC enables developers to develop, integrate, and test a target platform while the actual hardware system is still under development. Pre-integrated with ZebOS-XP control plane platform, ZebIC:

- Separates hardware development from software development through the ZebOS abstraction layer.
- Isolates all of the hardware and operating system specific interactions into a small set of well-defined function calls for the control plane.

ZebM. An IP Infusion product that allows network equipment manufacturers to develop management functionality for their networking products. ZebM provides a software framework and APIs for building on-device management systems for network equipment. The ZebM framework contains these core components:

- CML (Central Management Layer), transaction-oriented middleware that connects configuration and operational data on all management interfaces within a network device. CML is used by any northbound management application to manage ZebOS-XP or any third-party control plane.
- SMI (Simple Management Interface), a series of southbound Interface modules to connect with ZebOS-XP or any third party control plane protocol modules. SMI is the interface between the managed object and the CML.
- Model-driven northbound interface for automatic rendering of interfaces such as command-line interface (CLI) and NETCONF (Network Configuration Protocol).

ZebOS-XP. An IP Infusion product with Layer 2 (L2) and Layer 3 (L3) control plane software that allows network equipment manufacturers to rapidly add networking capabilities to communications products. ZebOS-XP is targeted at

manufacturers who provide solutions in carrier transport, access, Carrier Ethernet, mobile backhaul, data center, and cloud networking, including solutions for enterprise private clouds, hybrid clouds, and public clouds

The ZebOS-XP networking protocol modules conform to leading Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Metro Ethernet Forum (MEF), and other industry standards.