Global Knowledge™

Course Review Series

CCNA Review

CCNA Review

Rick Chapin, Global Knowledge Instructor

Note: This document is intended to help students understand what types of information would be required to pass the CCNA test. This is only intended as a review and additional training and knowledge would be needed in order to take and pass the CCNA exam. This document does not help with the simulation portion of the test.

OSI Reference Points

OSI Layer	Upper or Data Flow Layer	Network Reference	Network Device
Application	Upper		
Presentation	Upper		
Session	Upper	PDU or Message	
Transport	Data Flow	Segment	
Network	Data Flow	Packet or Datagram	MultiLayer Switch or Router
Data Link	Data Flow	Frame	Switch or Bridge
Physical	Data Flow	Bits and Signaling	Hub

OSI Layers

OSI Layer	Purpose	Examples
Application	Provides services to network applications. This layer is responsible for determining resource availability, identifying communications peers, and synchronizing communications between the applications.	• Simple Mail Transport Protocol (SMTP) • Telnet • File Transfer Protocol (FTP) • Trivial File Transfer Protocol (TFTP) • HyperText transfer Protocol (HTTP)
Presentation	Provides the coding and conversion functions that are applied to the data to/from the Application layer. This layer ensures that there is a common scheme used to bundle the data between the two ends. There are various examples and this list is by no means complete. Text can be either ASCII or EBCDIC. Images can be JPEG, GIF, or TIFF. Sound can be MPEG or Quicktime	• ASCII (text) • EBCDIC (text) • JPEG (image) • GIF (image) • TIFF (image) • MPEG (sound/video) • Quicktime (sound/video)
Session	Maintains communications sessions between upper-layer applications. This layer is responsible for establishing, maintaining, and terminating such sessions	• Session Control Protocol (SPC) • Remote Procedure Call (RPC) from Unix • Zone Information Protocol (ZIP) from AppleTalk

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Transport	Responsible for end-to-end data transmission. These communications can be either reliable (connection-oriented) or non-reliable (connectionless). This layer organizes data from various upper layer applications into data streams. The transport layer also handles end-to-end flow control, multiplexing, virtual circuit management, and error checking and recovery.	• Transmission Control Protocol (TCP) from IP • User Datagram Protocol (UDP) from IP
Network	Uses administrator-defined logical addressing to combine many data flows into an internetwork. This layer allows both connection-oriented and connectionless data flows to access the network. The network layer addresses help define a network hierarchy. Network devices are normally grouped together based on their common Network Layer address.	• Internet Protocol (IP)
Data Link	Provides either reliable or non-reliable transmission of data across a physical medium. Most networks use a non-reliable data link layer, such as Ethernet or Token Ring. The data Link Layer provides a physical address to each device called a Media Access Control (MAC) address. MAC addresses are typically burned into the network interface card (NIC). The Data Link Layer also uses a Logical Link Control (LLC) to determine the type of Network Layer data is traveling inside the frame.	LAN: • Ethernet/IEEE 802.3 (include Fast Ethernet) • 802.3z (Gigabit Ethernet) • Token Ring /IEEE 802.5 • FDDI (from ANSI) WAN: • High-Level Data-link Control (HDLC) • Point-to-Point Protocol (PPP) • Frame Relay
Physical	Defines the electrical, mechanical, and functional specifications for maintaining a physical link between network devices. This layer is responsible for such characteristics as voltage levels, timing and clock rates, maximum transmission distances, and the physical connectors used.	LAN: • Category 3 cabling (LAN) • Category 5 cabling (LAN) WAN: • EIA/TIA-232 • EIA/TIA-449 • V.35

Network Hierarchy

Layer	Purpose	Network Device
Core	To move network traffic as fast as possible. Characteristics include fast transport to enterprise services and no packet manipulation.	• High-speed routers • Multi-layer switches
Distribution	Perform packet manipulation such as filtering (security), routing (path determination), and WAN access (frame conversion). The distribution layer collects the various access layers. Security is implemented here, as well as broadcast and multicast control. Media translation between LAN and WAN frame types also occurs here.	• Routers
Access	Where end-stations are introduced to the network. This is the entry point for virtually all workstations.	• Switches • Bridges • Hubs

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

LAN Switch Functions

Function	Purpose
Address Learning	Dynamically learns MAC addresses that arrive in the switch by reading the sources MAC address of each arriving frame. If this address is not in the current MAC table, and there is enough space to store it, the address and the inbound port are stored.
Forward/Filter	Compare the destination MAC address of the arriving frame to the dynamically-learned MAC table. If the address is in the table only forward the frame out the port specified in the table, thus filtering it from other ports. If the MAC address is not in the MAC table (unknown MAC address) or it is a broadcast or multicast frame, the frame is flooded out every other port except the one it arrived from.
Loop Avoidance	Since the default behavior of a switch is to forward unknown unicast, broadcast, and multicast frames, it is possible for one frame to Loop endlessly through a redundant (multiple path) network. Thus the Spanning Tree Protocol (STP) is turned on to discourage loops in a redundant switch network.

Sources of Switching/Bridging Loops

Source	Description
Redundant Topology	Unknown Frames are flooded out all ports. If there are multiple paths, than a flood would go out all ports, except the originator, and come back in on the other ports, thus creating a loop.
Multiple Frame Copies	Two machines live (connect) on the same wire. They send frames to each other without assistance. If there are two bridges/switches attached to the same wire, who are also connected together, then new frames (unknown) going from one machine (same wire) would go directly to the other machine (same wire) and would also be flooded through the bridges/switches (connected wire) and be flooded back through the bridges/switches to the original wire. The receiving machine would receive multiple copies of the same frame.
MAC Database Instability	Thanks to a bridging/switching loop (senairo above), one bridge/switch learns the same MAC address on different ports. Thus, if a bridge/switch needed to forward a frame to its destination MAC address, it would have two possible destination ports.

Solution to Bridging/Switching Loops – 802.1d Spanning Tree Protocol

- Bridges/switches communicate with Bridge Protocol Data Units (BPDUs). The BPDU carries the Bridge ID and the Root ID
- Each bridge/switch has a unique Bridge ID, which is the priority (or priority and extend system ID) followed by the base MAC address of the bridge/switch. Only the priority (or priority and extend system ID) can be modified.
- The device with the lowest Bridge ID becomes the Root
- Only the Root is allowed to send BPDUs
- Initially, prior to receiving any BPDUs from other devices, every bridge/switch thinks it is the Root, and thus sends a BPDU to every other Bridge/switch. This always occurs when a new Bridge/switch is added to an existing network.
- After the round of BPDUs, every bridge/switch becomes aware of the lowest Bridge ID (the Root device). Only the Root continues to send BPDUs.
- BPDUs are sent, by default, every two (2) seconds.
- Every Bridge/switch receives BPDUs from the Root. If multiple BPDUs are received, then there must be a loop in the network. The BPDU with the lowest cost is the best path to the Root.
- The goal of every non-root bridge/switch is to find the most efficient path to the Root.
- Ports that are not the most efficient path to the root, and are not needed to reach any other downstream bridge/switch, are blocked. Blocked ports still receive BPDUs.
- If the primary path ceases to receive a BPDU, STP eventually forwards packets on an alternate port. Blocked ports are re-evaluated to find the most efficient and that port is un-blocked so a path can be reestablished to the root.

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

- Forwarding ports are also called Designated ports (DP).
- Blocked ports are also called non-Designated ports (BLK).
- The port that is forwarding to the Root is called the Root port (RP).
- The Root Bridge/switch ports never block and are always designated ports (DP).
- Bridge/switch convergence is the time between a break occurring and an STP calculating an alternate path. Typically 30 – 50 seconds.
- Port convergence is the time it takes for STP to calculate whether a port will be in forwarding or blocking mode. Typically 50 seconds.

Comparison of Bridges and Switches

Bridges	Switches
Software Based	Hardware-based (port-level ASICs)
Relatively Slow	Comparatively fast
One STP per Bridge	Possibly many STPs per switch (possibly one per VLAN)
Typically up to 16 Ports	Possibly hundreds of ports

Forwarding Modes in a Switch

Mode	Description	Latency
Store-and-Forward	The entire frame is buffered, the CRC is examined for errors and frame is checked for correct sizing (Ethernet 64 – 1518 bytes).	Relatively High. Varies depending on frame size.
Cut-Through	The frame is forwarded once the destination MAC address (first 6 bytes) arrives and is checked against the MAC address table. Buffer until the 6th byte arrives.	Lowest. Fixed delay based on 6 bytes being buffered. Not configurable on a Catalyst 1900.
Fragment-Free (Cisco)	The frame is forwarded once the first 64 bytes have arrived. Buffering occurs until the 64th byte arrives. Ethernet collisions usually occur within the first 64 bytes, thus if 64 bytes arrive there is no collision.	Low. Fixed delay based on 64 bytes being buffered. Default on Catalyst 1900.

Half-Duplex vs. Full-Duplex

Duplex Type	Advantages	Defaults
Half-Duplex	• Network devices us the same pair of wire to both transmit and receive • Only possible to use 50% of the available bandwidth – must use the same bandwidth to send and receive • Available bandwidth decreases as number of devices in the broadcast domain increases • Used through hubs (layer 1 devices) – everyone shares the available bandwidth	10 Mbps. 100 Mbps ports if not configured for full-duplex or cannot be Auto-sensed.
Full-Duplex	• Uses one pair of wire for sending and another pair for receiving. • Effectively provides double the bandwidth – possible to send and receive at the same time. • Must be point-to-point stations, such as pc/server-to-switch or router-to-switch. • Everyone has their own collision domain (individual bandwidth) on each switch port.	100 Mbps ports if manually configured for full-duplex or can be Auto-sensed

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

LAN Segmentation = Dividing Up the Size of Collision Domains

Device	Abilities
Bridge	Examines destination MAC address and makes filtering/forwarding decisions based on it. Unknown, Broadcast, and Multicast frames are flooded out all ports except the originator. Each port of a bridge is a collision domain.
Switch (VLANs)	Examines destination MAC address and makes filtering/forwarding decisions based on it. Unknown, Broadcast, and Multicast frames are flooded out all ports within that VLAN except the originator. Each port of a switch is a collision domain. Each VLAN is a broadcast domain. Benefits include simplifying moves, adds, and changes, reducing administrative costs, controlling broadcasts, tightened security, load distribution, and moving servers into a secure location.
Router	Examines destination network (logical – layer3) address and makes filtering/forwarding decisions based on it. Unknown and broadcast frames are discarded. Each port of a router is both a collision and broadcast domain.

TCP/IP Layers

Protocol	OSI Reference	Function
Transmission Control Protocol (TCP)	Session Layer – Layer 4	Reliable, connection-oriented, uses sequence and acknowledgement numbers to provide reliability verifies that the remote end is listening prior to sending data (handshake).
User Datagram Protocol (UDP)	Session Layer – Layer 4	Non-reliable, connectionless, no sequence or acknowledgement numbers, and no far-end verification.
Internet Protocol (IP)	Network Layer – Layer 3	Provides the logical addressing structure. Offers connectionless, best-effort delivery of packets (datagrams).

Port Numbers

Well-known port numbers are 1 – 1023 (typically used for well-known applications), random port numbers are 1024 and above (typically random numbers are used by the client in a client/server application).

Application	Port	Transport
File Transfer Protocol (FTP)	20/21	TCP
Telnet	23	TCP
Simple Mail Transfer Protocol (SMTP)	25	TCP
Domain Name Services (DNS)	53	TCP
Domain Name Services (DNS)	53	UDP
Trivial Files Transfer Protocol (TFTP)	69	UDP
Simple Network Management Protocol (SNMP)	161/162	UDP
Routing Information Protocol (RIP)	520	UDP

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

IP Protocols

Protocol	Purpose
Internet Control Message Protocol (ICMP)	Provides control and feedback messages between IP devices.
Address Resolution Protocol (ARP)	Using a destination IP address, ARP resolves or discovers the appropriate destination MAC (layer 2) address to use. Map a Layer 3 address to a Layer 2 address.
Reverse Address Resolution Protocol (RARP)	Using a source MAC address, RARP retrieves an IP address form the RARP Server. Map sources Layer 2 address to a Layer 3 address. RARP is an early form of BOOTP and DHCP.

IP Addresses

Class	First Binary Bits	Numerical Range	Number of Networks	Number of Hosts per Network	Number of Network Octets	Number of Hosts Octets
A	0xxx	1 – 126*	126	16.5 million	1 (N.H.H.H)	3
B	10xx	128 – 191	16 thousand	65 thousand	2 (N.N.H.H)	2
C	110x	192 – 223	2 million	254	3 (N.N.N.H)	1
D**	111x	224 – 239	N/A	N/A	N/A	N/A
E**	1111	240 – 255	N/A	N/A	N/A	N/A

* 127 is used for the Loopback address.

** Class D is used for Multicast Group addressing, and Class E is reserved for research use only.

Subnetting

Number of networks: $2^s - 2$, where s = number of bits in the subnet (masked) field

Number of hosts per subnet: $2^r - 2$, where r = number of host (non-masked) bits.

R + S = 32 (always), since there are 32 bits in an IP address and each bit is either a network or host bit. S is the bit(s) after the standard Class number of bits (Mask – Class Bits = S).

Subnet Masks

1s in the subnet mask match the corresponding value of the IP address to be Network bits

0s in the subnet mask match the corresponding value in the IP address to be Host bits

Default Subnet Masks

Default Class A mask – 255.0.0.0 = N.H.H.H

Default Class B mask – 255.255.0.0 = N.N.H.H

Default Class C mask – 255.255.255.0 = N.N.N.H

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Possible Subnet Mask Values for One Octet

Decimal Mask	Binary Mask	Network Bits	Host Bits
0	00000000	0	8
128	10000000	1	7
192	11000000	2	6
224	11100000	3	5
240	11110000	4	4
248	11111000	5	3
252	11111100	6	2
254	11111110	7	1
255	11111111	8	0

Possible Class C Subnet Masks

Decimal Mask	Network Bits (x)	Host Bits (y)	Number of Subnets $2^s - 2$	Number of Hosts $2^r - 2$
255.255.255.0	0	8	0	254
255.255.255.128	1	7	N/A	N/A
255.255.255.192	2	6	2	62
255.255.255.224	3	5	6	30
255.255.255.240	4	4	14	14
255.255.255.248	5	3	30	6
255.255.255.252	6	2	62	2
255.255.255.254	7	1	N/A	N/A
255.255.255.255	8	0	N/A	N/A

Routing

The process of maintaining a table of destination network addresses. A router will discard packets for unknown networks.

Sources of Routing Information

Source	Description
Static	• Manually configured by an administrator • Must account for every destination network • Each static route must be configured on each router • No overhead in processing, sending, or receiving updates • Saves bandwidth and router CPU • Routing table maintained by administrator
Dynamic	• A process that automatically exchanges information about available routes • Uses metrics to determine the best path to a destination network • The routing protocol must be configured on each router • Bandwidth is consumed as routing updates are transmitted between routers • Router CPU is used to process, send, and receive routing information • Routing table maintained by routing process

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Types of Routing Protocol

Type	Description
Interior	• Used within a common administrative domain called an Autonomous System (AS) • Typically a single AS is controlled by a single authority or company • Interior routing protocols are used within a corporate network
Exterior	• Used to connect Autonomous Systems • Exchanges routing information between different administrative domains • Exterior protocols are used to connect sites within a very large corporate network, or are used to connect to the Internet

Classes of Routing Protocol

Class	Description
Distance Vector	• Maintains a vector (direction and distance) to each network in the routing table • Typically sends periodic (update interval) routing updates • Typically sends entire routing table during update cycle • Routing updates are processed and then resent by each router, thus the updates are second-hand information (routing by rumor) • Typically prone to routing loops (disagreement between routers) and count to infinity (routing metrics continue to accumulate indefinitely) • Solutions to these problems include: - Spilt Horizon – do not send updates back to where they came from – eliminates back-to-back router loops - Define a maximum metric – eliminates count to infinity problem - Route poisoning – set the advertised metric to the maximum value on routes that have gone down - Poison reverse – overrides split horizon by informing the source of a route that it has gone down - Hold-down timers – eliminates long-distance loops by ignoring updates about "possibly down" routes that have metrics worse than the current metric - Triggered updates – send an individual update immediately when a route is thought to be down, rather than wait for the periodic update timer (also called flash updates)
Link State	• Maintains a complete topological map (database) of entire network, separate from the routing table (forwarding table) • Sends updates only when necessary • Only sends information that has changed, not the entire database • Does not send information from the routing table, but rather from the database • The initial routing update is sent to every link state router in the network (flooding) via a multicast IP address, not a processed copy as with distance vector protocols • Routing table is individually calculated on each router from its database. This process is called Shortest Path First or SPF • The database typically requires as much memory as the routing table • When SPF runs, it is CPU intensive • Uses "hello" packets to maintain a database of link state neighbors throughout the network

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Examples of Routing Protocols

Protocol	DV or LS	Internal or External	Characteristics
Routing Information Protocol (RIP)	DV	Internal	• Sends periodic updates every 30 seconds by default • Sends the entire routing table out every interface, minus the routes learned from that interface (split horizon) • Uses hop count as a metric • Has a maximum reachable hop count of 15 (16 is the defined maximum) • Sends updates out as a broadcast (RIP V1) • RIP V2 uses a multicast address of 244.0.0.10
Interior Gateway Routing Protocol (IGRP)	DV	Internal	• Sends periodic updates every 90 seconds by default • Sends the entire routing table out every interface, minus the routes learned from that interface (split horizon) • Uses a composite metric consisting of bandwidth, delay, reliability, load, and MTU • Only uses bandwidth and delay by default (configurable) • Does track hop count but only uses it as a tie-breaker • Default maximum hop count is 100, but is configurable up to 255 maximum • Sends updates out as a broadcast
Enhanced Interior Gateway Routing Protocol (EIGRP)	Adv. DV	Internal	• Considered an advanced distance vector routing protocol • Uses a Diffusing update algorithm (DUAL) • Sends triggered updates when necessary • Sends only information that has changed, not entire routing table • Uses a composite metric consisting of bandwidth, delay, reliability, load, and MTU • Only uses bandwidth and delay by default (configurable) • Does track hop count but only uses it as a tie-breaker • Default maximum hop count is 224, but is configurable up to 255 maximum • Sends updates out on a multicast address of 224.0.0.9
Open Shortest Path First (OSPF)	LS	Internal	• Sends triggered updates when necessary • Sends only information that has changed, not entire routing table • Uses a cost metric • Interface bandwidth is used to calculate cost (Cisco) • Uses two multicast addresses of 224.0.0.5 and 224.0.0.6
Border Gateway Protocol (BGP)	DV	External	• Actually a very advanced distance vector routing protocol • Sends triggered updates when necessary • Sends only information that has changed, not entire routing table • Uses a complex metric system

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Routing Configuration Commands

Type	Syntax
Static	Router(config)# ip route *dest-address subnet-mask next-hop* or *exit-interface* • *dest-network* is the network in question • *subnet-mask* is the network in question • *next-hop* is the network in question • *exit-interface* is the network in question - either the *next-hop* or *exit-interface* are used, but not both Example: Router# configure terminal Router(config)# ip route 172.16.0.0 255.255.0.0 serial0 or Router(config)# ip route 172.16.0.0 255.255.0.0 172.16.1.1
Dynamic	Router(config)# router protocol keyword Router(config-router) network network-number • *protocol* is the routing protocol being used • *keyword* is an optional parameter for some routing protocols • *network-number* is the directly connected network that will be used to send and receive routing updates; enables all interfaces that use that network address Example 1: Router# configure terminal Router(config)# router rip Router(config-router)# network 172.16.0.0 Router(config-router)# network 192.168.20.0 Example 2: Router(config)# router IGRP 100 Router(config-router)# network 172.16.0.0 Router(config-router)# network 192.168.20.0

Router Storage Locations

Memory Type	Contents
RAM	Operating environment
MVRAM	Backup (startup) copy of the configuration file, single file only
ROM	IOS subset (RxBoot) (only if the hardware supports it ROM Monitor (ROMMON)
Flash	Compressed IOS (non-compressed if 2500 series) Binary file storage capabilities (if enough space)
PCMCIA	Like Flash, some machines have multiple PCMCIA slots available
Share I/O	I/O buffer for interfaces

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Operating Modes of a Router

Mode	Prompt	Sample Functions
User	Router>	• Read-only privileges • Examine Interface status • Examine router status
Privileged	Router#	• Full privileges to read, write, modify, copy, and delete • Examine interface status • Examine router status • Examine configuration file • Change IOS and configuration file Example: Router> enable password password Router#
Configuration	Router(config)#	• Modify the active (running) configuration file Example: Router# configure terminal Router(config)#

Password Configuration

Mode	Location	Syntax
User	Console Port	Router# configure terminal Router(config)# line console 0 Router(config-line)# password string Router(config-line)# login
User	Auxiliary Port	Router# configure terminal Router(config)# line auxiliary 0 Router(config-line)# password string Router(config-line)# login
User	VTY Access	Router# configure terminal Router(config)# line vty 0 4 Router(config-line)# password string Router(config-line)# login
Privilege (enable)	N/A	Router# configure terminal Router(config)# enable password string
Privilege (secret)	N/A	Router# configure terminal Router(config)# enable secret string

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Some Miscellaneous IOS Commands

Function	Mode	Syntax
Configure a Banner	Config	Router(config)# banner motd # *banner #*
Configure the router name	Config	Router(config)# hostname *name*
Examine the backup configuration in NVRAM	Privileged	Router# show startup-config
Examine the active configuration in RAM	Privileged	Router# show running-config
Display the contents of Flash memory	User of Privileged	Router> show flash
Save the active configuration to NVRAM	Privileged	Router# copy running-config startup-config
Restore the backup configuration to RAM	Privileged	Router# copy startup-config running-config
Save the active configuration to a TFTP Server	Privileged	Router# copy running-config tftp
Restore a configuration file from a TFTP Server	Privileged	Router# copy tftp running-config
Write the current IOS out to a TFTP Server	Privileged	Router# copy flash tftp
Load a different IOS into the router	Privileged	Router# copy tftp flash
Erase the backup configuration from NVRAM	Privileged	Router erase startup-config
Boot using a different IOS in Flash	Config	Router(config)# boot system flash *filename*
Boot from a TFTP Server	Config	Router (config)# boot system tftp *ip-address filename*
Configure the router as a TFTP Server	Config	Router(config)# tftp-server flash *filename*
Reboot the router	Privileged	Router# reload
Use the setup utility	Privileged	Router# setup
Display directly-connected Cisco neighbors	User or Privileged	Router> show cdp neighbor
Display the command history buffer	User or Privileged	Router> show history
Configure the length of the history buffer	Privileged	Router# terminal history size *line-count*
Display the current IOS, router run-time, amount of memory, and interfaces installed	User or Privileged	Router> show version
Configure logout delay	Line Config	Router(config-line)# exec-timeout *minutes seconds*
Configure clocking on a DCE interface	Interface Config	Router(config-if)# clock rate *bps-value*
Configure the bandwidth on an interface	Interface Config	Router(config-if)# bandwidth *Kbps-value*
Display the IP routing table	User or Privileged	Router> show ip route
Display the physical characteristics of an interface	User or Privileged	Router> show interfaces *type number*
Display the logical characteristics of an interface	User or Privileged	Router> Show *protocol* interface *type number*

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Enhanced Editing Commands

Function	Syntax
Move to beginning of line	Ctrl-A
Move to end of line	Ctrl-B
Move back one word	Esc-B
Move forward one word	Esc-F
Move back one character	Ctrl-B or left arrow
Move forward one character	Ctrl-F or right arrow
Delete a single character	Ctrl-D or backspace
Recall previous command (up in buffer history)	Ctrl-P or up arrow
Move down through history buffer	Ctrl-N or down arrow

IP Access Lists

Type	Numbers	Criteria	Location
Standard	1 – 99	• Source IP address	Close to the destination
Extended	100 – 199	• Source IP address • Destination IP address • Source protocol number • Destination protocol number • Source port number • Destination port number	Close to the source
Expanded Standard	1300 – 1999	• Expanded number range	Close to the destination
Expanded Extended	2000 – 2699	• Expanded number range	Close to the source
Named	Alphanumeric string	• Same as standard extended or extended	Close to either destination or source

Access List Syntax

Direction	Description
Inbound	• Interrogates packets as they arrive, before they are routed • Can deny a packet before using CPU cycles to process it then deny it
Outbound	• Interrogates packets after they are routed to the destination interface • Packets can be discarded after they have been routed • Default configuration when applying access lists to the interface

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Direction	Description
Standard or Expanded Standard	Router(config)# access-list number permit or deny *source-ip wildcard-mask* • Number is in the range of 1-99, 1300-1999 • Each line either permits or denies • Only examines the sources IP address from the IP packet • Wildcard mask allows a single line to match a range of IP addresses • Default mask is 0.0.0.0 • Wildcard mask of 0.0.0.0 is exact match of source IP address • The word "host" can be substituted for the mask 0.0.0.0 • Wildcard mask of 255.255.255.255 means match every IP address • The word "any" can be substituted for the mask 255.255.255.255
Extended or Expanded Extended	Router(config)# access-list number permit or deny *source-ip source-mask operator source-port destination-ip destination-mask operator destination-port* • Number is in the range of 100 – 199, 2000 – 2699 • Each line either permits or denies • Examines anything in the IP header: source and destination addresses, protocols, and ports • Protocol can be IP, ICMP, IGRP, EIGRP, OSPF, UDP, TCP, and others • Wildcard mask allows a single line to match a range of IP addresses • Port numbers are optional and can only be entered if the protocol is UDP or TCP. Port numbers are in the range of 1 – 65535 • A protocol of ICMP, the port numbers becomes an ICMP type code • Operators are a Boolean function of gt, lt, neq, or range. LT is less than, GT is greater than, NEQ is not equal to, and RANGE is a range of ports • Boolean operators are only used with TCP or UDP • Wildcard mask of 0.0.0.0 is exact match of source IP address • The word "host" can be substituted for the mask 0.0.0.0 • Wildcard mask of 255.255.255.255 means match every IP address • The word "any" can be substituted for the mask 255.255.255.255
Named	Router(config)# access-list standard *name* Router(config-std-nacl)# permit or *deny source-ip wildcard-mask* or Router(config)# access-list extended *name* Router(config-ext-nacl)# permit or *deny source-ip source-mask operator source-port destination-ip destination-mask operator destination-port* • Same structure as Standard or Extended except alphanumeric string
Interface	Router(config-if)# ip access-group number in or out • Number is the access list being referenced; standard, extended, or named • In or out specifies the direction of the frame flow through the interface for the access list to be executed. Out is the default
Virtual Terminal (VTY)	Router(config)# line vty vt# or vty-range Router(config-line)# access-class number in or out • Restricts incoming or outgoing vty connections for address in access list • Number is the access list being referenced; standard, extended, or named

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Wildcard Masks

Mask	Match	Don't Care	Example
0.0.0.0	Every octet	N/A	172.16.10.1 = 172.16.10.1
0.0.0.255	First three octets	Last octet	172.16.10.1 = 172.16.10.0
0.0.255.255	First two octets	Last two octets	172.16.10.1 = 172.16.0.0
0.255.255.255	First octet	Last three octet	172.16.10.1 = 172.0.0.0
255.255.255.255	N/A	Every octet	172.16.10.1 = 0.0.0.0

Network Address Translation – NAT

Function	Syntax
Marks the interface as connected to the inside	Router(config-if)# ip nat inside
Marks the interface as connected to the outside	Router(config-if)# ip nat outside
Establishes static translation between an inside local address and an inside global address	Router(config)# ip nat inside source static *local-ip global-ip*
Defines a pool of global addresses to be allocated as needed	Router(config)# ip nat pool start-ip end-ip {netmask *netmask* | prefix-length *prefix-length*}
Establishes dynamic source translation to a pool based on the ACL	Router(config)# ip nat inside source list access-*list-number* pool name
Establishes dynamic source translation to a interface based on the ACL	Router(config)# ip nat source list access-*list-number* interface interface overload
Displays active translation	Router# show ip nat translations
Displays translation statistics	Router# show ip nat statistics
Clears all dynamic address translation entries	Router# clear ip nat translation *
Clears a simple dynamic translation entry that has an inside translation or both inside and outside translation	Router# clear ip nat translation inside *global-ip local-ip* [outside *local-ip global-ip*]
Clears a simple dynamic translation entry that has an outside translation	Router# clear ip nat translation outside *local-ip global-ip*
Clears an extended dynamic translation entry	Router# clear ip nat translation protocol inside *global-ip global-port local-ip local-port* [outside *local-ip local-port global-ip global-port*]

WAN Connection Types

Connection	Definition
Leased Line	• A pre-established, private connection from one site to another through a provider's network • Also called a dedicated circuit or a dedicated connection • Always a point-to-point connection between two end points • Used when there is a constant flow of data, or when a dedicated amount of bandwidth is required • One router interface is connected to one destination site • Examples – PPP, HDLC

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Connection	Definition
Circuit Switching	• A dial-up connection through a provider's voice-grade network • Either uses an analog modem or an ISDN connection • Used when only a slow-speed connection is needed, or when there is not much of a need to transfer a lot of data • One call establishes a circuit to one destination site • Examples – PPP, HDLC, SLIP
Packet Switching	• Each site only uses one physical connection into the provider's network, however there may be multiple virtual circuits to various destinations • Typically less expensive than leased lines, because you are mixing various data streams across a single link • Used when a dedicated connection is needed, but cost savings is important • Examples – Frame Relay, X.25
Cell Switching	• Each site only uses one physical connection into the provider's network, however there may be multiple virtual circuits to various destinations • Typically less expensive than leased lines, because you are mixing various data streams across a single link • Uses fixed-size packets called cells to achieve faster and more predicable transport through the network • Examples – ATM, SMDS
High-Level Data Link Control (HDLC)	• A Cisco-proprietary serial encapsulation • Allows multiple network-layer protocols to travel across • Default encapsulation for all serial interfaces on a Cisco router • One router interface only goes to one destination
Point-to-Point Protocol (PPP)	• An open-standard serial encapsulation • Allows multiple network-layer protocols to travel across • Allows optional link-layer authentication (CHAP or PAP) • One router interface only goes to one destination
Serial Line Internet Protocol (SLIP)	• An open-standard serial encapsulation • Allows only IP to travel across • One router interface only goes to one destination
Frame Relay	• A very popular packet switching standard • Uses switched virtual circuits (SVCs) or permanent virtual circuits (PVCs) • Allows multiple network-layer protocols to travel across • Each virtual circuit is a private channel between two end points • One router interface may have many virtual circuits, going to the same location or various locations
X.25	• An old, but still available, packet switching standard • Uses switched virtual circuits (SVCs) or permanent virtual circuits (PVCs) • Allows multiple network-layer protocols to travel across • Each virtual circuit is a private channel between two end points • One router interface may have many virtual circuits, going to the same

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Popular WAN Terms

Term	Definition
Customer Premise Equipment (CPE)	• Network devices/equipment physically located at the customer's location/site • Customer is typically required to procure/maintain this equipment • Equipment could include routers and CSU/DSUs
Central Office (CO)	• The facility that provides WAN services to the customer • Source of analog phone service, ISDN service, DSL service, frame relay connections, X.25 connections, and leased lines
Local Loop	• The link from the provider's CO to the customer's demarc • Also called the "last mile" • Normally not more than a few miles
Demarcation Point (Demarc)	• The line between the customer site and the provider network • Inside of the demarc is the CPE • Outside of the demarc is the local loop
Toll Network	• The provider's network • Inside the WAN cloud • Typically "smoke and mirrors" to a customer

ISDN Device Types

Device	Function
Network Termination 1 (NT-1)	Converts BRI signals into a form used by the ISDN digital line
Network Termination 2 (NT-2)	The aggregation point of ISDN services at a customer site
Terminal Adapter (TA)	Converts analog signals into BRI signals
Terminal Endpoint 1 (TE-1)	A devices that has an ISDN interface, such as a router
Terminal Endpoint 2 (TE-2)	A device that does not have any ISDN interfaces and requires a TA to access the ISDN network, such as a PC

ISDN Reference Points

Reference Point	Function
R	The point between a non-ISDN device and the TA
S	The point between the TA and the NT-2, or between ISDN devices and the NT-2
T	The point between the NT-2 and the NT-1
U	The point between the NT-1 and the ISDN provider

ISDN Protocols

Reference Point	Function
E-series	Recommend telephone network standards
I-series	Deal with concepts, terminology, and general methods used within ISDN
Q-series	Cover switching and signaling through the ISDN cloud

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

ISDN Interface Types

Interface Type	Characteristics
Basic Rate Interface (BRI)	• 2 Bearer (B) channels, 64 Kbps data each • 1 control channel (D), 16 Kbps
Primary Rate Interface (PRI)	• 23 Bearer (B) channels, 64 Kbps data each – across a T1 circuit, typically seen in North America and Japan • 30 Bearer (B) channels, 64 Kbps data each – across an E1 circuit, typically seen in Australia and Europe • 1 control channel (D), 64 Kbps

Sample ISDN Commands

Function	Mode	Syntax
Configure the ISDN switch type	config	Router(config)# isdn switch-type *switch* • switch types include basic-dms100, basic-5ess and basic-ni
Create a static route	config	Router(config)# ip route *network mask destination-ip* • network is the other side of the ISDN cloud, since there is no dynamic routing protocol running across the ISDN network • mask is the subnet mask to specify the distant network • destination-IP is the IP address of the BRI interface of the remote site
Create a dialer list	config	Router(config)# dialer-list *number* protocol *protocol* permit • number can be from 1 – 10 • protocol can be any protocol, such as IP or IPX
Access the BRI interface	config	Router(config)# interface bri *number*
Assign SPID numbers	interface config	Router(config-if)# isdn spid1 *spid-number* • spid-number is the logical circuit ID assigned by the ISDN provider • there might be two SPID numbers, thus the second one would be referenced as "spid2"
Reference the dialer list	interface config	Router(config-if)# dialer-group *number* • number is the dialer list created earlier
Create a map to point to and dial the remote site	interface config	Router(config-if)# dialer map *protocol destination-ip dial-number* • protocol is the protocol being mapped across the ISND cloud, such as IP or IPX • destination-IP is the IP address of the BRI port on the other side of the ISDN cloud, specified by the static route • dial-number is the ISDN phone number of the remote site

Frame Relay Terms

Term	Definition
Local Access Rate	Connection rate between a frame relay site and the frame relay provider. Many virtual circuits run across a single access point.
Virtual Circuit	Logical connection between two end points • Permanent Virtual Circuit (PVC) – the circuit is always available, and the bandwidth for the circuit is always allocated • Switched Virtual Circuit (SVC) – the circuit is built when needed, and the bandwidth is returned when the circuit is closed

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Term	Definition
Data Link Connection Identifier (DLCI)	The local reference to one end of a virtual circuit. The DLCI numbers are assigned by the frame relay providers.
Committed Information Rate (CIR)	The maximum allowed bandwidth through the PVC from one end to the other. Each PVC can have a unique CIR.
Inverse Address Resolution Protocol (IARP)	The process of a frame relay device, such as a router, discovering the network-layer information about the devices at the other end of the PVCs.
Local Management Interface (LMI)	Signaling between the frame relay device (the router) and the frame relay switch (the provider). LMI does not travel across the entire PVC from one end to the other.

Sample Frame Relay Commands

Function	Mode	Syntax
access the serial interface	config	Router(config)# interface serial *number*
change the encapsulation	interface config	Router(config-if)# encapsulation frame-relay *option* • option can either be Cisco (default) or ietf (open standard)
specify the LMI type	interface config	Router(config-if)# frame-relay lmi *lmi-type* • lmi-type can be Cisco, ansi, or q933a • this command is normally not needed, as the router will automatically sense the LMI type if configured by the provider
assign the local DLCI	interface config	Router(config-if)# frame-relay interface-dlci *local-dlci* • local-dlci is the DLCI number of the PVC that terminates on this interface. There can be more than on DLCI on an interface. • this command is not needed with a major interface, since the router will automatically retrieve the DLCIs from the frame relay switch.
create a sub-interface	config	Router(config)# interface serial *number.sub* point-to-point or multipoint • point-to-point defines a subinterface that will only have one DLCI (interface-dlci command) • multipoint defines a subinterface that may have more than one DLCI (interface-dlci command)
create a static map	interface config	Router(config)# frame-relay map *protocol destination-IP local-dlci* • protocol is the protocol being mapped across the frame relay cloud, such as IP or IPX • destination-IP is the IP address of the frame relay interface at the other end of the PVC • local-DLCI is the local DLCI needed to access the remote site • this command is not needed if inverse-ARP is properly configured, and the interface-dlci command is used

Configuration Register

8 4 2 1	8 4 2 1	8 4 2 1	8 4 2 1	binary weight
15 14 13 12	11 10 9 8	7 6 5 4	3 2 1 0	bit position
0 0 1 0	0 0 0 1	0 0 0 0	0 0 1 0	bits set
2	1	0	2	hex value

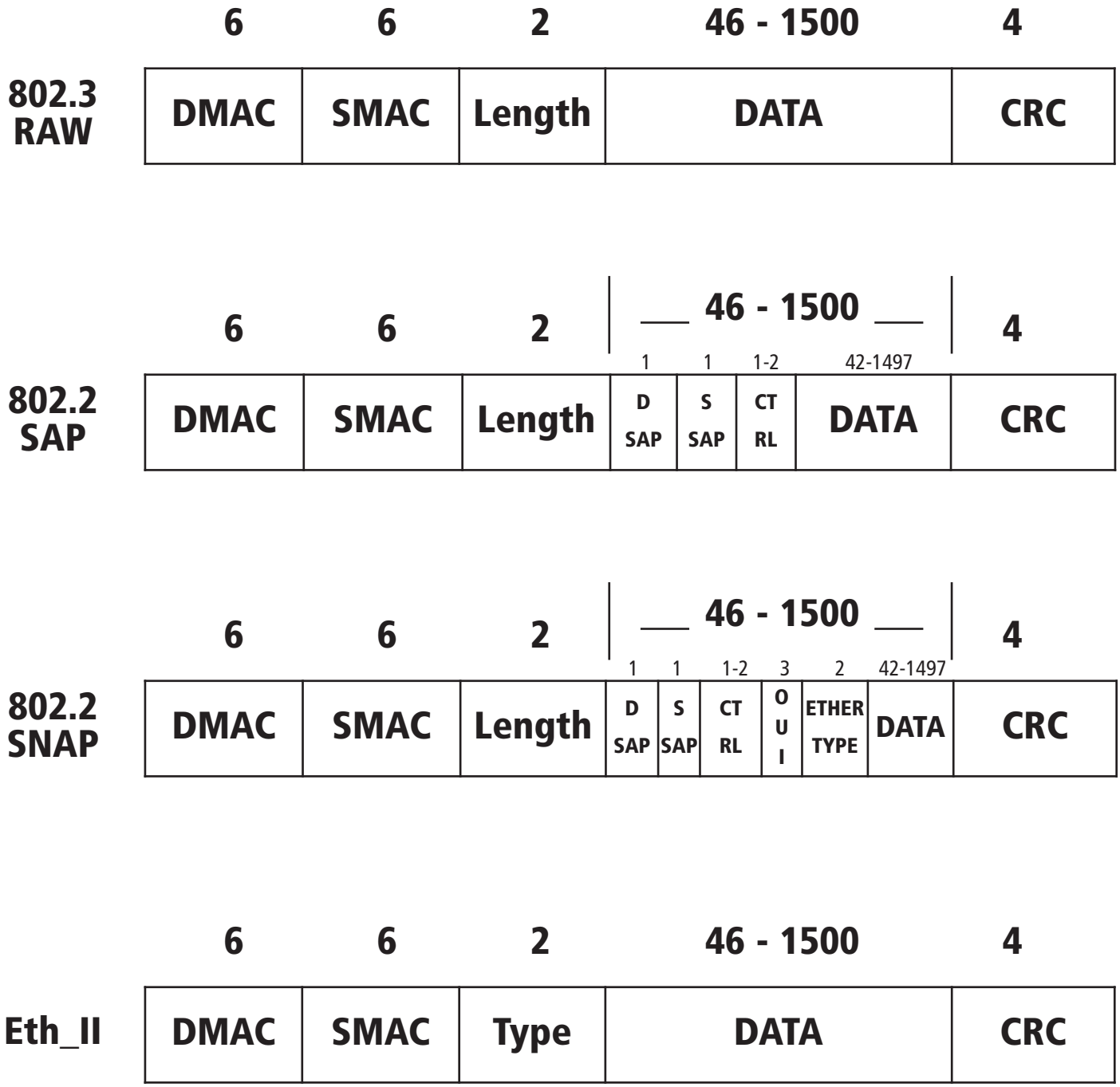
Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Bit# Description of Configuration Register Bits

15	Diagnostic mode display and Ignore NVRAM (11.x): 0 = disable, 1 = enable
14	Broadcasts of network field: 0 = ones, 1 = network number
13	Boot ROMs or BOOTFLASH if network boot fails: 1 = yes, 0 = no
12-11	Console speed: 00 = 9600, 01 = 4800, 10 = 1200, 11 = 2400
10	IP broadcasts of ones or zeros: 0 = ones, 1 = zeros
09	Use Secondary Bootstrap: 0 = disable, 1 = allow
08	Break key: 1 = disable, 0 = allow
07	OEM display disable: 0 = display, 1 = no display
06	Ignore NVRAM: 0 = disable, 1 = enabled
05	Change baud rate up to 115.2k on 1600, 1700, 2600, and 3600, use with bits 12 & 11 001 = 19.2, 011 = 57.6, 101 = 38.4, 111 = 115.2 Note: bit order is 12, 11, 5
04	Bypass bootstrap loader (fast boot): 0 = disable, 1 = enable
03-00	Boot field: 0 = MONITOR, 1 = ROM/BOOTFLASH IOS, 2-F = NETBOOT

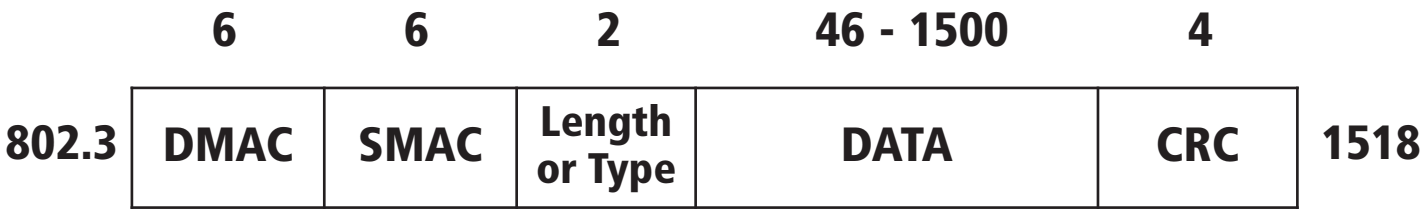
Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Ethernet Frame Types



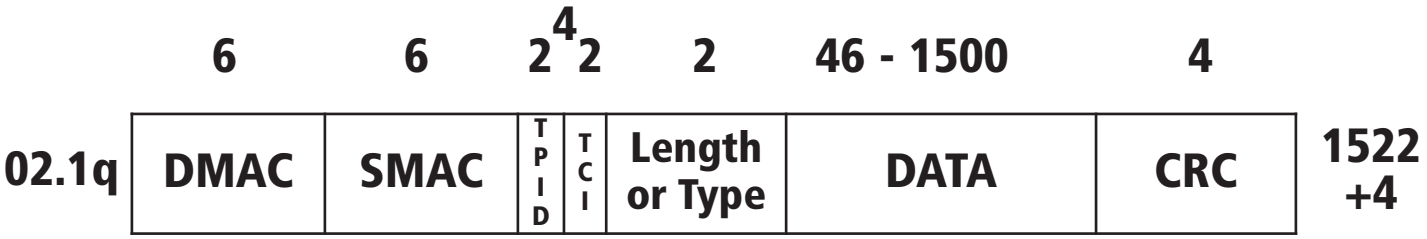
Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

ISL Frame Types



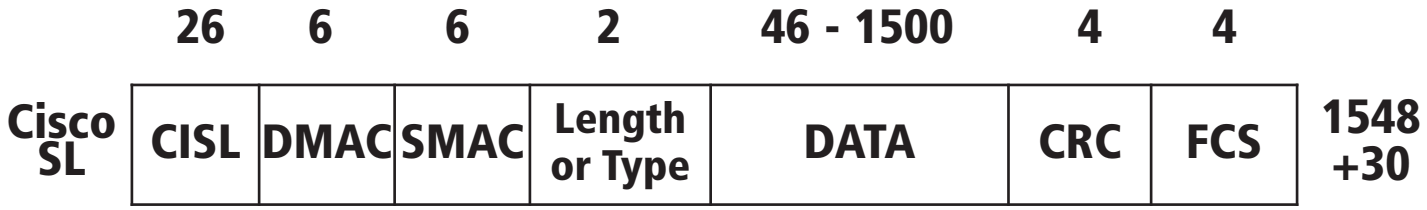
LENGTH (Field value shows length of packet) - 0x0001 - 0x05DC (1 - 1500 bytes)

TYPE (Field value shows type of protocol being carried) - 0x05DD - 0xFFFF



TPID (Type Identifier) - 0X8100 - ISL Packet

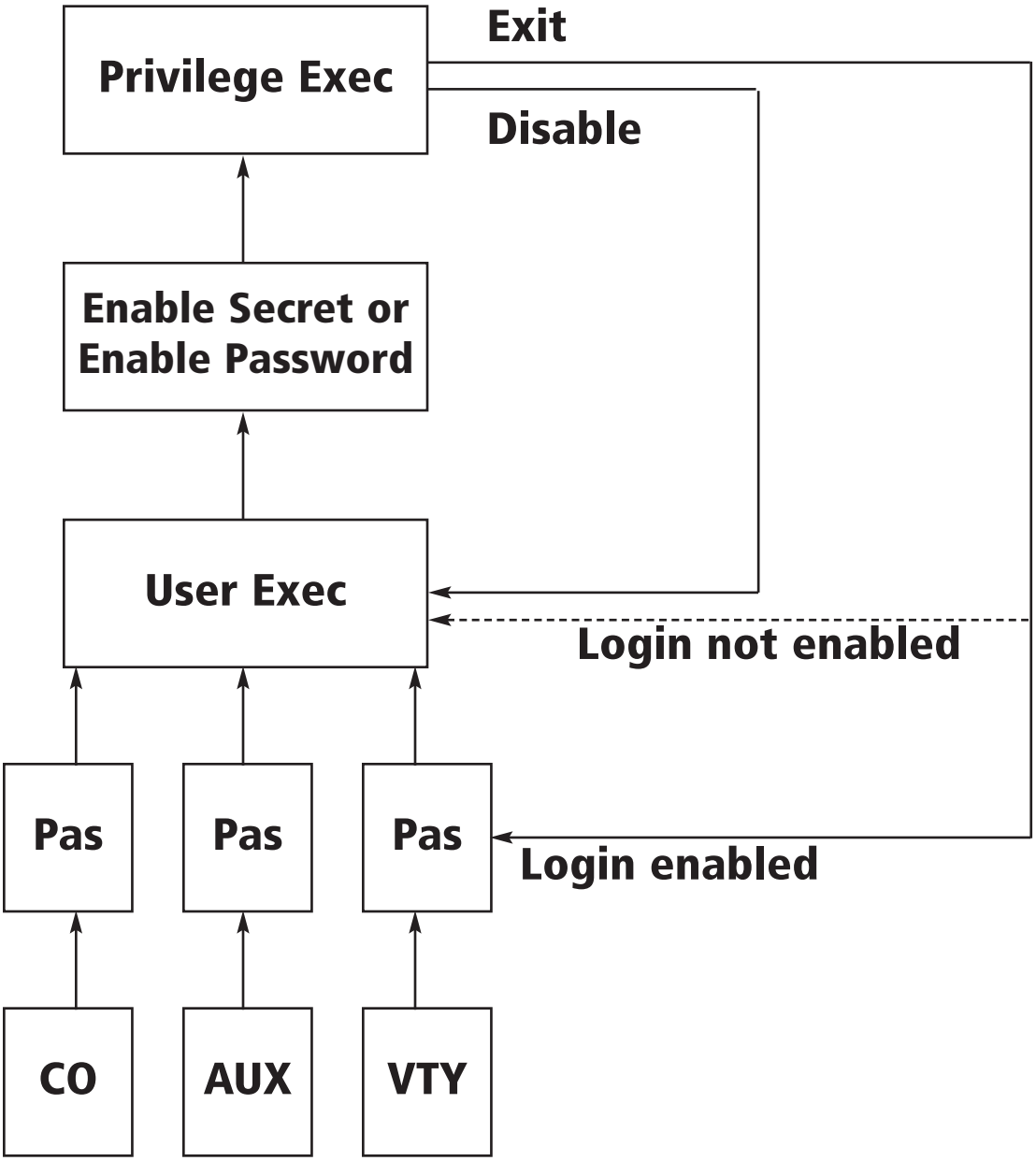
TCI (Tag Control Information) - 3 bits for priority
- 1 bit for format (canonical vs.non-canonical)
- 12 bits for Vlan ID



CISL (Cisco ISL) - 1 bit for BPDU/CDP (Bridge Packet Data Unit/Cisco Discovery Protocol)
- 15 bits for Vlan ID

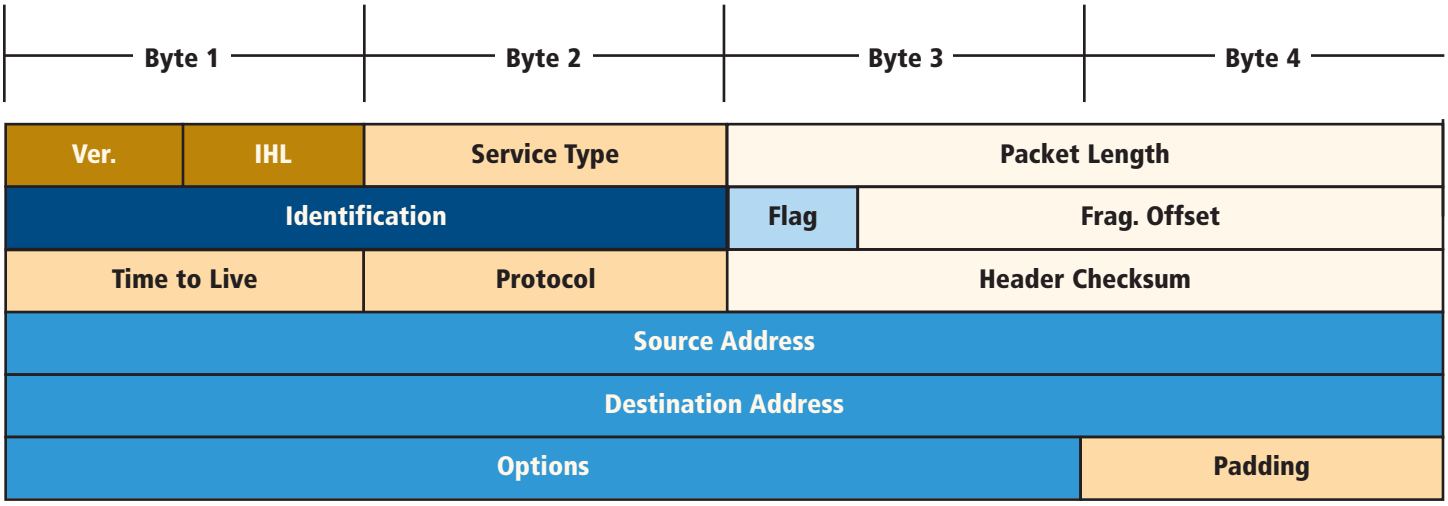
Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Password Flow Chart

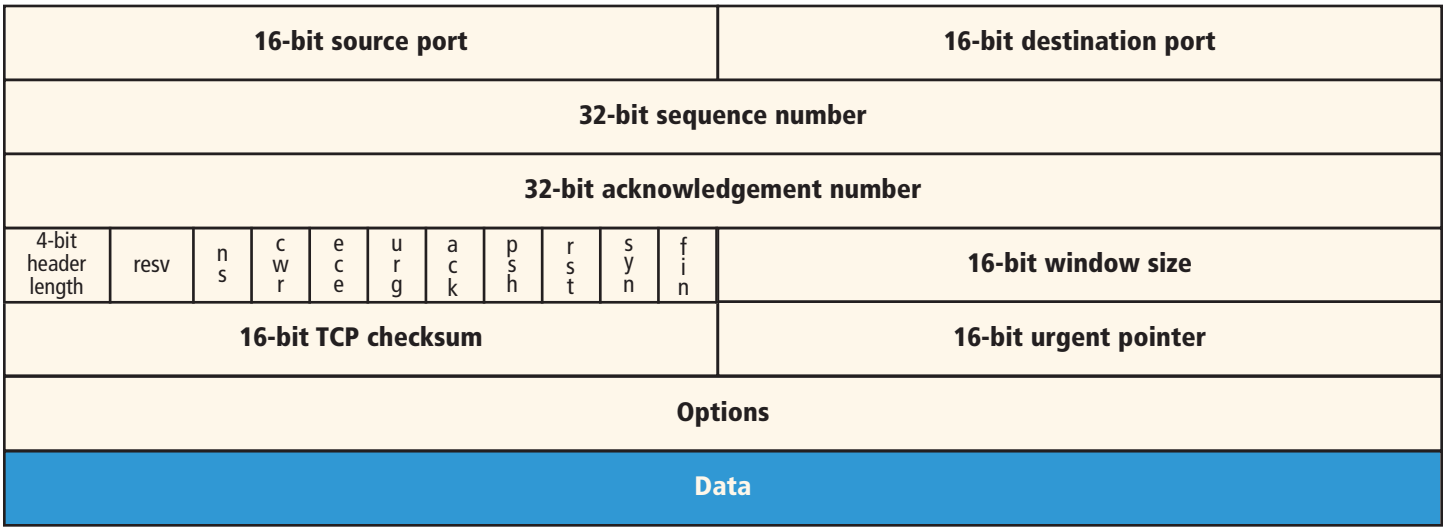


Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

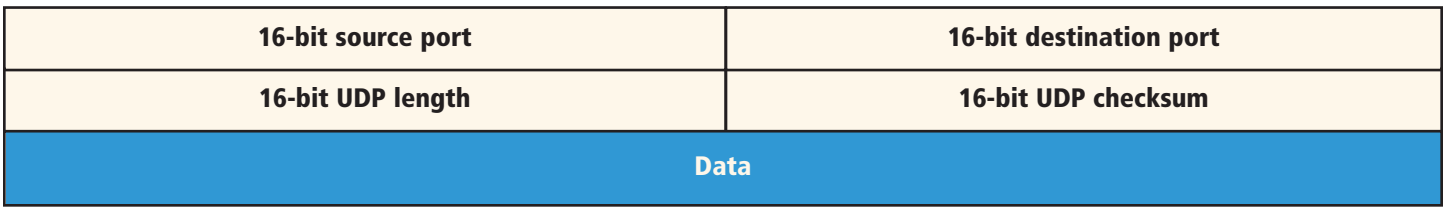
IP Header



TCP Header



UCD Header



Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge course:

CCNA® Boot Camp

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative.

Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 700 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and management training needs.

About the Author

Rick Chapin teaches a variety of Cisco classes for Global Knowledge including INTRO, ICND, CCNA Boot camp, CIT, BSCI, BCMSN, BCRAN, BGP, and Voice classes. His real-world experience includes working with large companies such as Digital Equipment Corporation, Control Data Corporation, IRS, NASA, EPA, and Cisco Systems.

Copyright ©2005 Global Knowledge Network, Inc. All rights reserved.