

Cisco CCENT, CCNA, CCNP (CCIE)

© Copyright 2020

Document name : Communication Cisco CCxx.docx

Last update: 01.10.2020

Author: Albert Balogh

Table of Content

Introduction	13
Certification	13
Cisco Certified Entry Network Technician (CCENT®)	15
Cisco Certified Network Associate Routing and Switching (CCNA®)	16
Cisco Certified Network Professional (CCNP®)	16
Cisco Certified Internetwork Expert (CCIE®)	17
Cisco Certified Systems Instructor (CCSI®)	17
Authorities	17
Network Design Steps	18
Cable Questions	18
Analyze a Network	19
Multinode Core	20
Multi-Tier Architecture	21
Three-Tier Architecture	22
Two-Tier Architecture	22
Typical Components of an Enterprise Network	23
CORE-Layer (Backbone)	23
Distribution-Layer	25
Access-Layer	25
Switch Block	25
Leaf-Spine Network Topology	26
Routing Protocol Considerations	27
Routing Protocol Migration	27
IPv6 Migration	27
Network Summarization	27
Network Maintenance Plan	27
Asynchronous Routing	27
Out of order packets	27
Troubleshooting Models	28
Hierarchical Network Design	28
Flat Network Topology	28
OSI-Layers	28
Physical Layer (Layer 1)	30
Data Link Layer (Layer 2)	30
Network Layer (Layer 3)	30
Transport Layer (Layer 4)	30
Session Layer (Layer 5)	30
Presentation Layer (Layer 6)	31
Application Layer (Layer 7)	31
INTERNETWORKING	32
Network Segmentation	32
Possible causes of LAN Traffic Congestion	32
HUB	32
Switch	32
Configuring Switch	32
Troubleshooting Switch	33

Bridge	33
Router.....	33
Configuring Router	34
Troubleshooting Router.....	34
CEF - Cisco Express Forwarding	34
Brouter.....	35
Repeaters.....	35
Token Ring Hub	36
Token Ring - Frame Format	36
IOS License Management	36
Cisco Wireless LAN Controllers (WLCs)	37
Wireless Access Point (AP, IEEE 802.11)	37
Cisco Wireless Access Points	37
Same-Layer interaction	37
Adjacent-Layer interaction	37
Bandwidth Delay Product (BDP)	37
Path Maximum Transmission Unit Discovery (PMTUD)	38
DSLAM - Digital Subscriber Line Access Multiplexer	38
ETHERNET NETWORKS.....	39
Encapsulation.....	39
Collision Domain	40
Broadcast Domain.....	40
CSMA/CD.....	40
Ethernet Cabling	40
MAC-Address.....	41
OUI - Organizationally Unique Identifier.....	41
MAC-Address Table (CAM).....	42
TCAM	42
TCP/IP	43
IP - Internet Protocol	44
IGMP - Internet Group Management Protocol	44
CIDR - Classless Inter-Domain Routing	44
IPv4	44
Classful Network Concept.....	44
Private IPv4 Address Spaces	45
IPv4 Multicast Addresses.....	45
APIPA - Automatic Private IP Addressing.....	46
Unicast	46
Unicast Flooding.....	46
Broadcast	46
Interface Naming Conventions.....	47
Global Synchronization / TCP Synchronization	47
End-to-End Delay.....	47
Troubleshooting: Latency/Packet-Loss.....	47
Troubleshooting: TCP/IP.....	48
Network Related Registry.....	48
Frequent Asked Questions (FAQ)	50
EASY SUBNETTING	51
Subnet-Zero	51
Supernet.....	52
VARIABLE LENGTH SUBNET MASK (VLSM)	52
INTERNETWORKING OPERATING SYSTEM (IOS)	53
The IOS File System	53
Router Boot Sequence.....	53
Router Modes.....	53
Setting Passwords	54
Configuring SSH	56
Configuring SSH for VTY Access	56
Troubleshooting Interfaces	56
Troubleshooting Serial Lines	56
ROUTER SECURITY CONCEPTS	57
Router Security Policy.....	57
Passwords	57

Authentication.....	57
Access.....	57
Services.....	57
Filtering.....	57
Routing Protocols.....	58
Backups.....	58
Documentation.....	58
Redundancy.....	58
Monitoring.....	58
Updates.....	58
RBAC - Role-Based Access Control.....	58
Routing Protocol Authentication.....	58
Authentication Methods.....	58
Key Chains.....	58
EIGRP Authentication.....	59
OSPF Authentication.....	60
BGP Authentication.....	60
BGP IPv6 Authentication.....	61
Access Control Lists.....	61
uRPF - Unicast Reverse Path Forwarding.....	61
uRPF Modes.....	61
Configuring uRPF.....	61
Troubleshooting uRPF.....	61
AAA - Authentication, Authorization and Accounting.....	62
Authentication.....	62
Authorization.....	62
Accounting.....	62
Configuring AAA.....	62
Troubleshooting AAA.....	63
SNMP Security.....	63
MANAGING A CISCO INTERNETWORK.....	64
INTERNAL COMPONENTS OF A CISCO ROUTER AND SWITCH.....	64
The Purpose of the Configuration Register.....	64
Dynamic Host Configuration Protocol (DHCP).....	65
DHCP Options.....	65
Configuring DHCP.....	65
Configuring DHCP-Relay.....	66
Troubleshooting DHCP.....	66
Network Time Protocol (NTP).....	66
Configuring NTP.....	67
Troubleshooting NTP.....	67
NTP Authentication.....	67
CDP - Cisco Discovery Protocol.....	67
Link Layer Discovery Protocol (LLDP).....	68
Telnet.....	69
IP ROUTING.....	70
Static Routing.....	70
Default Routing.....	71
Dynamic Routing.....	71
Routing Protocols.....	71
Distance Vector.....	71
Link State.....	71
Path Vector Protocol.....	72
Hybrid- / Advanced Distance Vector.....	72
Administrative Distance (AD).....	72
RIPv1.....	72
RIPv2.....	73
RIPng.....	73
Configuring RIPng.....	74
Troubleshooting RIPng.....	74
IS-IS.....	74
Troubleshooting ROUTES.....	74
EVN - Cisco Easy Virtual Network.....	75

LAYER 2 SWITCHING	76
Address learning	76
Forward/filter decision	76
EtherChannel	76
Configuring EtherChannel	77
Troubleshooting EtherChannel	77
PortFast	77
UplinkFast	77
BackboneFast	78
BPDU Guard - Bridge Protocol Data Unit Guard	78
BPDU Filtering	78
Root Guard	78
Port Security	78
Configure Port-Security	79
Troubleshooting Port-Security	80
LAN-Switching	80
Store-and-Forward	80
Transparent Bridging	80
Multilayer Switching	81
Route caching	81
Topology based	81
Configuration Catalyst Switch	81
Troubleshooting Catalyst Switch Configuration	81
PoE - Power over Ethernet	83
Configuring PoE	83
Troubleshooting PoE	83
VIRTUAL LANs (VLANs) and INTER VLAN ROUTING	83
Frame Tagging	84
VLAN Identification Methods	84
VLAN Membership	84
Configuring VLANs	85
Configuring Trunk Ports	85
Configuring Router on a Stick (ROAS)	85
Configuring Inter-VLAN Routing	86
Switched Virtual Interface (SVI)	86
TCAM	86
Configuring SVI	87
Troubleshooting SVI	87
VoIP - Data and Voice VLANs	87
Configuring Data and Voice VLAN	88
Private VLANs (PVLANS)	88
Troubleshooting VLAN	88
Administrative Modes	90
Operational Modes (Actual status)	91
VLAN Trunk Protocol (VTP)	91
VTP versions	91
VTP Domains	92
VTP Modes	92
VTP Pruning	92
Configure VTP database mode	92
Troubleshooting VTP	93
SECURITY	94
Access Control Lists (ACLs)	94
Router Access Control Lists (RACLs)	94
VLAN Access Control Lists (VACLs)	94
Port Access Control Lists (PACLs)	95
Layer 4 Operators (L4 Ops)	95
Standard access lists	95
Extended access lists	95
Named access lists	96
Time-Based ACLs	96
Infrastructure ACLs	96
Context-Based ACLs (CBAC)	96

Configure ACLs	96
Troubleshooting ACLs	97
NAT - NETWORK ADDRESS TRANSLATION	98
Types of Network Address Translation	98
NAT Names	100
Configuring NAT	100
Troubleshooting NAT	101
@INTERNET PROTOCOL VERSION 6 (IPv6)	102
IPv6 fragmentation	103
IPv6 Naming Conventions	103
Global Unicast Address (2001:....)	105
Configure a global unicast address	105
Configure a global IPv6 address with autoconfigured IP address	105
Global unicast address (2000::/3)	106
Link-local Addresses (FE80::/10)	106
Configure a static link-local address	106
Unique Local Address (FC00::/7)	106
Multicast (FF00::/8)	107
Anycast	107
Manual Address Assignment	107
Solicited Node Multicast address (FF02::1:FF00:0/104)	107
SLAAC - Stateless Address Auto Configuration	107
Configuring SLAAC	108
Modified Extended Unique Identifier (EUI-64) Method	108
DHCPv6 (Stateful Dynamic Addressing)	109
IPv6 Header	109
ICMPv6	110
Neighbor Discovery (NDP)	111
NDP NS/NA	111
NDP RS/RA	112
Router Solicitation (RS)	112
Router Advertisement (RA)	112
Duplicate Address Detection (DAD)	112
Inverse Neighbor Discovery (IND)	112
IPv6 Routing Protocols	113
Static Routing with IPv6	113
Transition Strategies	113
6to4 Tunneling	113
Configuring IPv6	114
Troubleshooting IPv6	114
ENHANCED SWITCHED TECHNOLOGIES	115
Spanning Tree Protocol (STP, IEEE 802.1D)	115
Spanning Tree Algorithm (STA)	116
Root Bridge Election	118
Root Bridge Placement	119
Configuring STP	119
Troubleshooting STP	120
Troubleshooting STP Protection	120
Loop Guard	120
UDLD - Unidirectional Link Detection	120
Normal Mode	121
Aggressive Mode	121
Rapid STP (RSTP, 802.1w)	121
PVRST+	121
MST - Multiple STP	121
MSTP+	121
MANAGING CISCO DEVICES	122
Integrated Services Router (ISR)	122
DHCP Snooping	122
RADIUS - Remote Authentication Dial-in User Service	122
Configuring RADIUS	122
Troubleshooting RADIUS	123
TACACS+ - Terminal Access Controller Access Control System	123

Configuring TACACS+	123
Troubleshooting TACACS+	123
Diameter	123
Switch Stacking	123
Cisco FlexStack/FlexStack-Plus	124
FHRP - First-Hop Redundancy Protocols	125
HSRP - Hot Standby Router Protocol	125
Configuring HSRP	126
Troubleshooting HSRP	126
VRRP - Virtual Router Redundancy Protocol	126
Configuring VRRP	128
Troubleshooting VRRP	128
GLBP - Gateway Load Balancing Protocol	128
Configuring GLBP	128
Toubleshooting GLBP	128
IP SERVICES	129
Syslog / Logging	129
Logging Categories (dinwecae)	129
Debug Command	130
Cisco Network Services (CNS)	130
Simple Network Management Protocol (SNMP)	130
SMIv1/SMIv2 Structure of Management Information Version X	131
Management Information Base (MIB)	132
NetFlow	132
Configuring NetFlow	133
Troubleshooting NetFlow	134
Per-Destination Load Balancing	134
Per-Packet Load Balancing	134
TROUBLESHOOTING IP, IPv6	135
IP SLA - IP Service-Level Agreement	135
Configuring IP SLA ICMP Echo	136
Troubleshooting IP SLA ICMP Echo	137
UDP	137
UDP Dominance	137
Jitter	137
Low Latency Queuing (LLC)	138
Helpdesk Templates	138
TROUBLESHOOTING VLANs	139
IGRP	139
Troubleshooting IGRP	139
EIGRP	139
Split Horizon	140
Poison Reverse	140
The three major steps	140
Reliable Transport Protocol (RTP)	142
Diffusing Update Algorithm (DUAL)	142
EIGRP Metrics	142
Configuring EIGRP	142
Troubleshooting EIGRP	143
EIGRPv6	144
Configuring EIGRPv6	145
Troubleshooting EIGRPv6	145
Named EIGRP	145
Configuring Named EIGRP	146
Troubleshooting Named EIGRP	146
OPEN SHORTEST PATH FIRST (OSPF)	147
Stub network	152
Configuring STUB	153
Troubleshooting STUB	153
Configuration NSSA	154
Configuration Totally NSSA	154
The OSPF Exchange Process	154
OSPF Route Filtering	154

Type-3 LSA Filtering.....	154
Loopback Interfaces.....	155
Configuring Loopback Interfaces.....	155
Troubleshooting Loopback Interfaces.....	155
Wildcard Mask.....	155
Configuring OSPF.....	155
Troubleshooting OSPF.....	156
OSPFv3.....	158
OSPFv3 Address Family Configuration.....	158
Configuring OSPFv3.....	158
Troubleshooting OSPFv3.....	159
MULTI-AREA OSPF.....	159
Adjacency Requirements.....	160
Configuring Multi-Area OSPF.....	160
Troubleshooting Multi-Area OSPF.....	160
BORDER GATEWAY PROTOCOL (BGP).....	161
BGP Transit AS.....	162
iBGP - Internal BGP.....	163
Configuring iBGP.....	163
Troubleshooting iBGP.....	163
eBGP - External BGP.....	163
Configuring eBGP.....	163
Troubleshooting eBGP.....	164
Single-Homed (1 link per ISP, 1 ISP).....	164
Dual-Homed (2+ links per ISP, 1 ISP).....	164
Single-Multihomed (1 link per ISP, 2+ ISPs).....	165
Dual-Multihomed (2+ links per ISP, 2+ ISPs).....	165
BGP Path Attributes (PA).....	166
Decision Steps.....	166
Peer Groups.....	168
Configuring BGP.....	168
Troubleshooting BGP.....	169
Multiprotocol BGP (MP-BGP).....	170
Configuring MP-BGP.....	170
Troubleshooting MP-BGP.....	171
WIDE AREA NETWORKS (WANs).....	172
WAN Connection Bandwidth.....	172
WAN Connection Types.....	174
WAN Protocols.....	175
ATM - Asynchronous Transfer Mode.....	175
Cable.....	175
Cellular 3G.....	175
Cellular 4G.....	175
Cellular 5G.....	175
Cisco Intelligent WAN (IWAN).....	175
Cisco Long Range Ethernet (LRE).....	175
Frame Relay.....	175
FTTx - Fiber to the x.....	177
SDLC - Synchronous Data Link Control.....	177
HDLC - High -Level Data -Link Control.....	177
HSSI - High Speed Serial Interface.....	178
ISDN.....	178
Metro Ethernet (MetroE).....	178
MPLS.....	178
P2P - Peer-to-Peer.....	179
PPP - Point-to-Point Protocol.....	179
SMDS - Switched Multimegabit Data Service.....	180
L2F - Layer 2 Forwarding Protocol.....	181
L2TP - Layer 2 Tunneling Protocol.....	181
PPTP - Point-to-Point Tunneling Protocol.....	181
PPPoE - PPP over Ethernet.....	181
PPP over ATM (PPPoA).....	182
RAN - Radio Access Network.....	182

VSAT	182
xDSL	182
Route Redistribution	182
Configuring Redistribution	184
Troubleshooting Redistribution	185
Route Selection	185
Policy-Based Routing (PBR)	185
Virtual private dial-up networks (VPDNs)	185
Troubleshooting VPDN	186
Virtual Routing and Forwarding (VRF)	186
Configuring VRF:	187
Troubleshooting VRF:	187
VRF-Lite	187
Configuring VRF-Lite:	187
Multi-VRF	187
Configuring Multi-VRF:	187
Next Hop Resolution Protocol (NHRP)	187
Configuring NHRP	188
Troubleshooting NHRP	188
Apple Networks	188
AppleTalk	188
LocalTalk	188
AppleShare	188
EtherTalk	188
TokenTalk	188
CABLING	190
SDN - Software Defined Networking	191
YANG	191
REST	192
Cisco APIC-EM	192
Functions:	192
Pros:	193
Southbound API (Cisco ACI)	193
Path Trace App	193
Quality of Service (QOS)	193
HCI - Hyperconverged Infrastructure	194
SDN Solutions	194
OpenDaylight	194
OpFlex	194
OpenFlow	194
UCS - Cisco Unified Computing System	194
I2RS - Interfaces to the Routing System	195
SDDC - Software Designed Datacenter	195
@INTERNET CONNECTIVITY	196
Static IP Address Assignment	196
Dynamic IP Address Assignment	196
IPv6 INTERNET CONNECTIVITY	196
Methods of Assigning an IPv6 Address	196
Methods of Assigning an IPv6 Address to a CPE	197
Manual Configuration	197
Stateless Address Autoconfiguration (SLAAC)	197
Stateless DHCPv6	197
DHCPv6 Prefix Delegation (DHCPv6-PD)	197
Single Session versus Dual Session	197
Single IPv4 BGP Session	197
Dual IPv4/IPv6 BGP Session	197
IPv6 Access Control List	197
IPv6 @Internet Connection Security	197
VPN	198
IPSec - IP Security VPN's	198
Troubleshooting IPSec	198
Secure Sockets Layer (SSL) - VPN's	198
S-HTTP - Secure Hypertext Transfer Protocol	199

GRE - Generic Routing Encapsulatio (GRE Tunnel)	199
Multipoint GRE (mGRE)	200
Cisco Dynamic Multipoint VPN (DMVPN)	201
DMVPN Phase I (Spoke-to-Hub only)	201
DMVPN Phase II (Spoke-to-Spoke)	201
DMVPN Phase III (Spoke-to-Spoke)	201
Configuring DMVPN	201
Troubleshooting DMVPN	202
Cisco Easy VPN	202
Cisco Group Encrypted Transport VPN (GETVPN)	202
Cisco Secure Socket Layer VPN (SSLVPN)	202
Domain Name System (DNS)	202
Ping (ICMP)	202
Traceroute / Tracert	203
IPv4 Routing	203
Point-to-Point-WANs	203
Leased Line (Serial Connection)	203
Overlay Transport Virtualization (OTV)	204
CISCO PRODUCTS	205
CISCO ACS	205
CISCO DUO	205
CISCO HyperFlex Systems (HX)	205
Cisco HyperFlex Systems Stretched Cluster	206
CISCO ISE	206
CISCO MERAKI	207
Configuring Authentication Proxy:	207
CISCO Prime	207
CISCO Security MARS	207
CISCO Stealthwatch	207
CISCO Umbrella	207
Cisco IOS Command Reference (CLI)	209
*** A ***	209
*** B ***	209
*** C ***	209
*** D ***	210
*** E ***	211
*** F ***	211
*** G ***	211
*** H ***	211
*** I ***	211
*** J ***	212
*** K ***	212
*** L ***	212
*** M ***	213
*** N ***	213
*** O ***	213
*** P ***	213
*** Q ***	213
*** R ***	213
*** S ***	213
*** T ***	217
*** U ***	218
*** V ***	218
*** W ***	218
*** X ***	218
*** Y ***	218
*** Z ***	218
Standard: Latency	220
Latency for SAP	220
Latency for MS Dynamics AX / Axapta	220
Latency for MS Navision (NAV)	220
Latency for VoIP	220
Tools: Looking Glass (@Internet)	220

NETWORK TECHNIQUES.....	221
464XLAT	221
Address Resolution Protocol (ARP).....	221
Akamai Technologies Inc.....	221
APNIC	221
Archie	222
ArcNet	222
Autonomous System Number (ASN).....	222
Broadcast Domain.....	223
CAPWAP.....	223
Certificate Types	223
Certificate Authority (CA)	224
Private Key and Certificate.....	224
System Configuration	224
Cipher	225
Cisco Application Visibility and Control (AVC).....	225
Cloud Solution	225
Public Cloud	225
Private Cloud	225
Hybrid Cloud.....	225
Community Cloud	225
Collision Domain	225
CSR-File Extension.....	226
Dark Fibre	226
Denial-of-Service (DoS)	226
DNSBL	226
DNS Round Robin load balancing	227
Domain Name System Security Extensions (DNSSEC).....	227
Dynamic DNS (DDNS)	227
ECHELON.....	227
Economic Operators Registration and Identification (EORI) System	227
Enhanced Data rates for GSM Evolution (EDGE)	228
Fibre Channel (FC)	228
Fibre Channel over Ethernet (FCoE)	228
File Systems.....	228
Frame Relay.....	228
FTP.....	228
FTPS	228
Gopher	228
High-Speed Downlink Packet Access (HSDPA)	229
High-Speed Uplink Packet Access (HSUPA).....	229
HTML.....	229
HTTP.....	229
Hub and Spoke	229
IBM Websphere Application Server (WAS)	229
Internet Relay Chat (IRC).....	229
Internet Content Adaption Protocol (ICAP).....	230
IoT - Skydrive and Rackspace Cloud.Internet of Things	230
ISATAP.....	230
Jumbo Frames	230
Koppelnetz / Coupling Network.....	231
Layer 2 VPN	231
Layer 3 VPN.....	232
Lightweight Third-Party Authentication (LTPA).....	232
Link Aggregation Control Protocol (LACP)	232
Metro Ethernet Forum (MEF)	232
Maximum Transmission Unit (MTU)	232
Multiprotocol Label Switching (MPLS)	233
Nagles's Algorithm	233
NAT-PT for IPv6.....	233
NetBIOS over TCP/IP (NBT, NetBT).....	234
Network Address Translation (NAT)	235
Network Address Translation 64 (NAT64)	235

Network Prefix Translation version 6 (NPTv6).....	236
Network Device Enrollment Service (NDES)	236
Network Policy Server (NPS)	236
Network TAP	237
Network News Transfer Protocol (NNTP)	237
Payload	237
PIP.....	237
PKCS.....	237
Port Trunking.....	238
Proxy Automatic Config (PAC).....	238
Rack - Mounted Automatic Transfer Switch (ATS)	238
RARP - Reverse Address Resolution Protocol.....	238
RIPE Network Coordination Centre (NCC)	238
Routing Information Protocol (RIP)	239
RTP - Real Time Transport Protocol.....	239
Simple Certificate Enrollment Protocol (SCEP)	239
Small form-factor pluggable transceiver (SFP)	239
Types.....	240
Software as a Service (SaaS).....	240
Cisco Cloud Web Security (prev. ScanSafe).....	241
Spanning Tree Protocol (STP, IEEE 802.1D).....	241
Split tunneling.....	241
Advantages.....	241
Disadvantages.....	241
SRTP - Secure Real Time Transport Protocol.....	241
Synchronous Optical Networking (SONET)	242
Symmetric Digital Subscriber Line (SDSL)	242
Server Hosting	242
Server Housing	242
Server Message Block (SMB 3.0).....	242
Switched Port Analyzer (SPAN).....	242
Configuring SPAN	242
Remote Catalyst Switched Port Analyzer (RSPAN)	243
Configuring RSPAN.....	243
SMTP	243
Split-Brain.....	244
SMLT - Split Multi Link Trunk.....	244
Squid	244
SSLvX	244
Switching.....	244
Layer 1.....	244
Layer 2.....	244
Layer 3.....	244
Layer 4.....	245
Layer 5.....	245
Layer 7.....	245
Tail-Drop	245
TCP/IP Stack (OSI & TCP-Model)	245
Telnet	245
Teredo.....	245
Time Zones / Zeitzone.....	246
TINA VPN Tunnel.....	246
Trusted Platform Module (TPM).....	246
Transport Layer Security (TLS).....	246
Universal Mobile Telecommunications System (UMTS).....	247
Variable-Length Subnet Masking (VLSM).....	247
Very-high-bit-rate Digital Subscriber Line (VDSL or VHDSL)	247
Virtual LAN (VLAN)	247
VLT - VLAN-Trunk.....	248
VxLAN - Virtual Extensible LAN	248
VSAT - Very Small Aperture Terminal	248
Firewall Types	248
Circuit-Level Firewall	248

Stateful Inspection Firewall	248
NGFW - Next Generation Firewall.....	249
Packet Filtering Firewall	249
WAF - Web Application Firewall.....	249
Placemet Decision Tree	250
BorderWare Firewall Server 6.1	250
Checkpoint One.....	250
Fortinet	250
IPTables	250
NOKIA	251
SonicWALL.....	251
TIS Firewall Toolkit.....	251
Watchguard	251
WEBRTC - Web Real-Time Communication	251
WLAN	251
Autonomous Mode	252
Lightweigts Mode.....	252
2.4 GHz-Frequenzband.....	252
5 GHz-Frequenzband	252
WPA	253
WPA2	253
WWW	253
X.509 PKI	253
XFP Transceiver (XFP)	253
RFCs.....	254
DEFINITIONS	256
ACI - Application Centric Infrastructure.....	256
CCP - Cisco Container Platform	256
COPS - Common Open Policy Service.....	256
SDA - Software Defined Access	256
Secure routing protocols	256
DWDM - Dense Wavelength Division Multiplexing	256
Split DNS - Split Domain Name System	256
Abbreviations	258
Table of Figures	260
Index	262

Introduction

For training the “Cisco Learning Labs” can be used.

<http://www.learnisco.net/test-ccna.php?exam=100-105>

www.lammle.com
www.lammle.com/forum
www.lammlesim.com

www.sybex.com/go/ccnarssg
www.sybex.com/go/ccentsg

www.cisco.com/web/learning
www.cisco.com/en/US/products/hw/routers/index.html
<http://www.cisco.com/techsupport>

Simulator: **IOS CCNA RS Simulator** or **LammleSim IOS**
IOS_CCENT_SimulatorSetup.exe

<http://www.boson.com/netsim-cisco-network-simulator> Chargeable
www.pearsonitcertification.com/networksimulator

Certification

www.vue.com
<http://www.pearsonvue.com/cisco/>
<http://www.learnisco.net/test-ccna.php?exam=100-105>
<http://www.learnisco.net/test-ccna.php?exam=200-105>

<https://learningnetwork.cisco.com/docs/DOC-25129>

<https://learningnetwork.cisco.com/docs/DOC-25128>

CCNA R/S 200-120

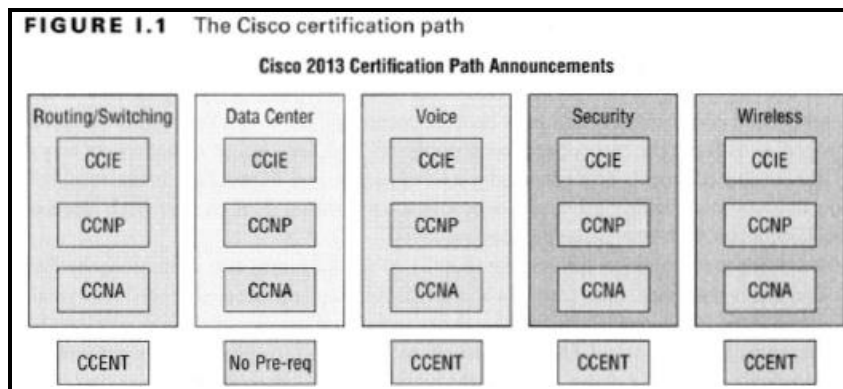
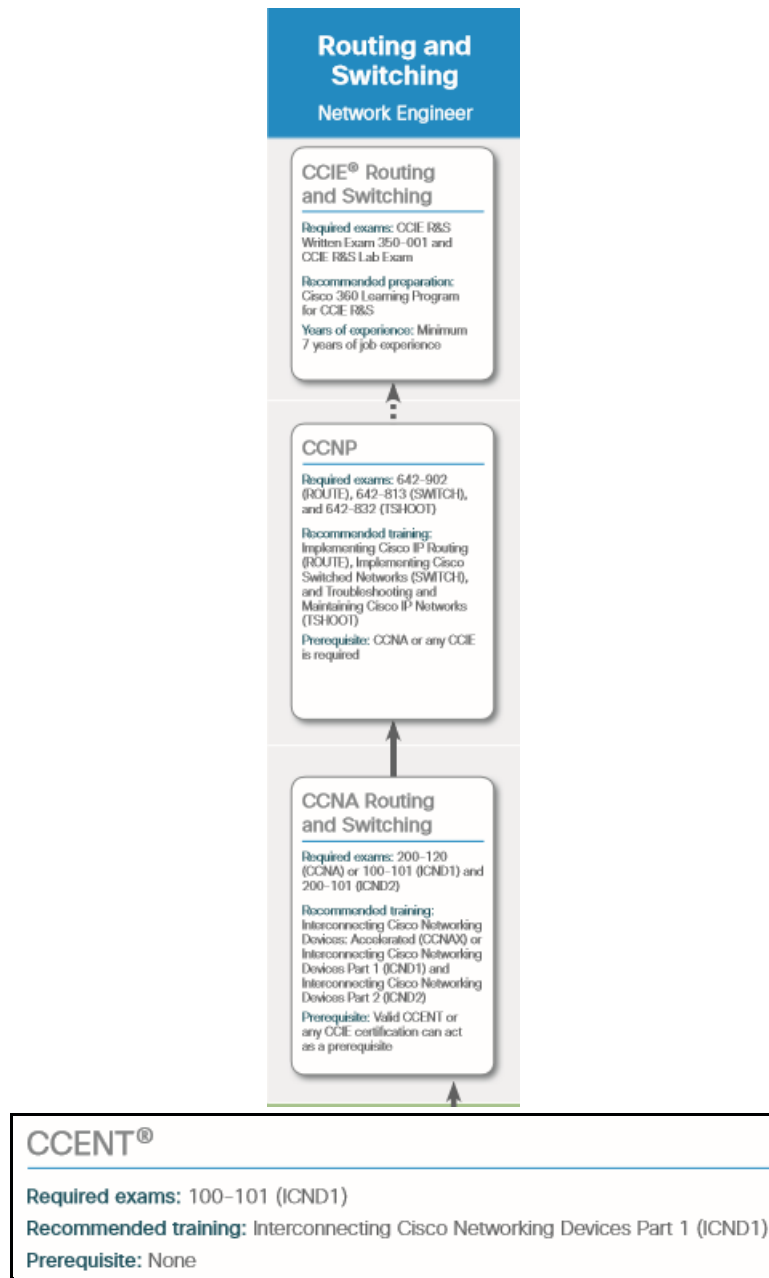


Figure 1: Cisco Certification Path

	Entry	Associate	Professional	Expert
Architect				CCAr Architect
Cloud		CCNA Cloud	CCNP Cloud	
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration
Cybersecurity Operations		CCNA CyberOps		
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center
Design	CCENT	CCDA	CCDP	CCDE
Industrial / IoT		CCNA Industrial		
Routing & Switching	CCENT	CCNA Routing and Switching	CCNP Routing and Switching	CCIE Routing and Switching
Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Service Provider		CCNA SP	CCNP SP	CCIE SP
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Other Certifications	Certified Technician			
Specialist	Business	Data Center	Internet of Things	Network Programmability
	Security	Operating System Software	Service Provider	Collaboration

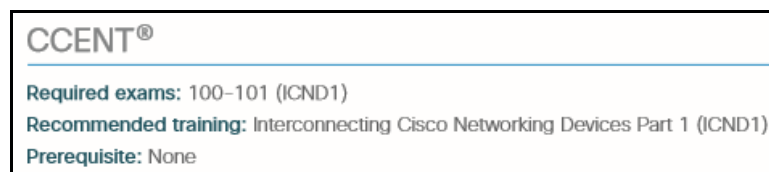


Cisco Certified Entry Network Technician (CCENT®)

ICND1 100-105 Interconnecting Cisco Networking Devices Part 1

<http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/entry/ccent.html>

The **CCENT** certification validates the skills required for entry-level network support positions, the starting point for many successful careers in networking. CCENT certified professionals have the knowledge and skill to install, operate, and troubleshoot a small enterprise branch network, including basic network security.



Cisco Certified Network Associate Routing and Switching (CCNA®)

ICND2 200-101

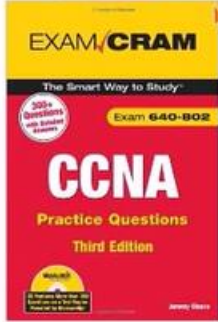
CCNA Routing and Switching

Required exams: 200-120 (CCNA) or 100-101 (ICND1) and 200-101 (ICND2)

Recommended training:
Interconnecting Cisco Networking Devices: Accelerated (CCNAX) or Interconnecting Cisco Networking Devices Part 1 (ICND1) and Interconnecting Cisco Networking Devices Part 2 (ICND2)

Prerequisite: Valid CCENT or any CCIE certification can act as a prerequisite

CCNA Practice Questions (Exam 640-802) and over 950,000 other books are available for Amazon Kindle - A



Click to **LOOK INSIDE!**


CCNA Practice Questions (Exam 640-802) (3rd Edition)
Jeremy Cleara (Author)
★★★★☆ (15 customer reviews) | Like (0)

List Price: ~~\$24.99~~
Price: **\$19.99** & eligible for **FREE Super Saver Shipping** on orders
You Save: **\$5.00 (20%)**

In Stock.
Ships from and sold by Amazon.com. Gift-wrap available.

Want it delivered Thursday, June 9? Order it in the next 6 hours and 34 minutes to get **One-Day Shipping** at checkout. [Details](#)

39 new from \$13.39 **13 used** from \$10.99

 **FREE Two-Day Shipping for Students.** [Learn more](#)

Cisco Certified Network Professional (CCNP®)

See: www.cisco.com/go/ccnp

Videos: https://learningnetwork.cisco.com/community/learning_center/ccnp-routing-switching-training-videos

CCNP

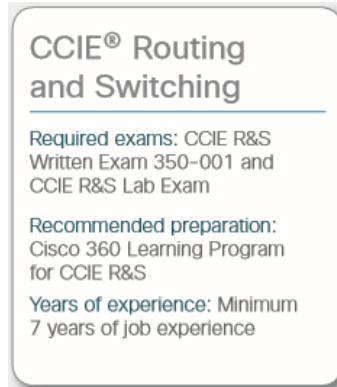
Required exams: 642-902 (ROUTE), 642-813 (SWITCH), and 642-832 (TSHOOT)

Recommended training:
Implementing Cisco IP Routing (ROUTE), Implementing Cisco Switched Networks (SWITCH), and Troubleshooting and Maintaining Cisco IP Networks (TSHOOT)

Prerequisite: CCNA or any CCIE is required

Exams	
Required Exam(s)	Recommended Training
300-101 ROUTE	Implementing Cisco IP Routing (ROUTE) v2.0
300-115 SWITCH	Implementing Cisco IP Switched Networks (SWITCH) v2.0
300-135 TSHOOT	Troubleshooting and Maintaining Cisco IP Networks (TSHOOT) v2.0

Cisco Certified Internetwork Expert (CCIE®)



Exams	
Required Exam(s)	Recommended Training
CCIE Routing and Switching Written Exam (400-101)	Implementing Cisco Quality of Service (QoS) Implementing Cisco MPLS (MPLS) IPv6 Fundamentals, Design and Deployment (IP6FD) Additional Study/Learn information for the Written Exam

Cisco Certified Systems Instructor (CCSI®)

Authorities

ICANN The **Internet Corporation for Assigned Names and Numbers** (www.icann.org) owns the processes by which public IPv6 and IPv6 addresses are allocated and assigned.

IANA The **Internet Assigned Numbers Authority** (www.iana.org) carries out many of ICANN's policies. IANA allocates address ranges to **Regional Internet Registries (RIR)**.
See: www.iana.org/numbers
IP Address Range allocation to RIRs
ASN Allocation

RIR **Regional Internet Registries (RIR)** subdivides the address space by allocating public address ranges to **National Internet Registries (NIR)** or **Local Internet Registries (LIR)**. ISPs are typically LIRs.

AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe the Middle East and Central Asia

LIR **Local Internet Registries (LIR)**
A local Internet registry (LIR) is an organization that has been allocated a block of IP addresses by a regional Internet registry (RIR), and that assigns most parts of this block to its own customers. Most LIRs are Internet service providers, enterprises, or academic institutions. Membership in a Regional Internet registry is required to become an LIR.

IR Each type of **Internet Registry (IR)** can assign a further subdivide range of addresses to the end-user organization to use.

See also: www.potaroo.net

Network Design Steps

- What is the **number of sites** connected to the network
- What is the **number of routers**
- What is the **number of adjacent neighbors**
- Keep your **"Broadcast Domains"** as small as possible
- Keep an eye on router processing / **routing tables**
- Consider **route summarization** in the subnet design.
- Check out the Cisco CVD's → www.cisco.com/go/cvd
- Fibre wiring** is commonly used in **mesh** and **ring topologies**
- What is the expected **frequency of changes** on **access layer**
- What is the expected **frequency of changes** on **distribution layer**
- What is the expected **frequency of changes** on **core layer**
- Design the network around **traffic flows** rather than a particular **type of traffic**,

Access / Distribution Switch Level

FHRP HSRP, VRRP, GLBP

Core

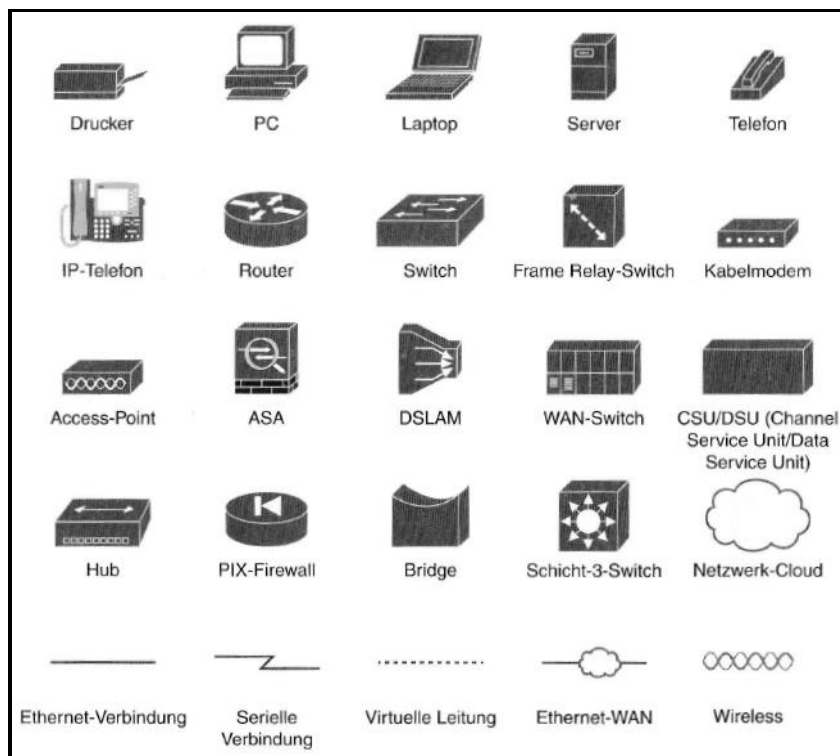
FHRP HSRP, VRRP, GLBP

Layer 2 Etherchannel

Routing Distance Vector (RIP, IGRP, EIGRP)

Link State (OSPF, IS-IS)

Path Vector Protocol (BGP, BGP-4, MP-BGP)



Cable Questions

The most common causes of network failure are cable failures or misconfigurations.

- Is the router being connected to a data terminal equipment (DTE) or data communication equipment (DCE) device?
- Is a male or female connector required on the cable?
- What signaling standard does the device require?
- To group switches using a special cable (**stack port**)

Analyze a Network

```
#show interfaces  
#show interfaces status  
#show vlan
```

Multinode Core

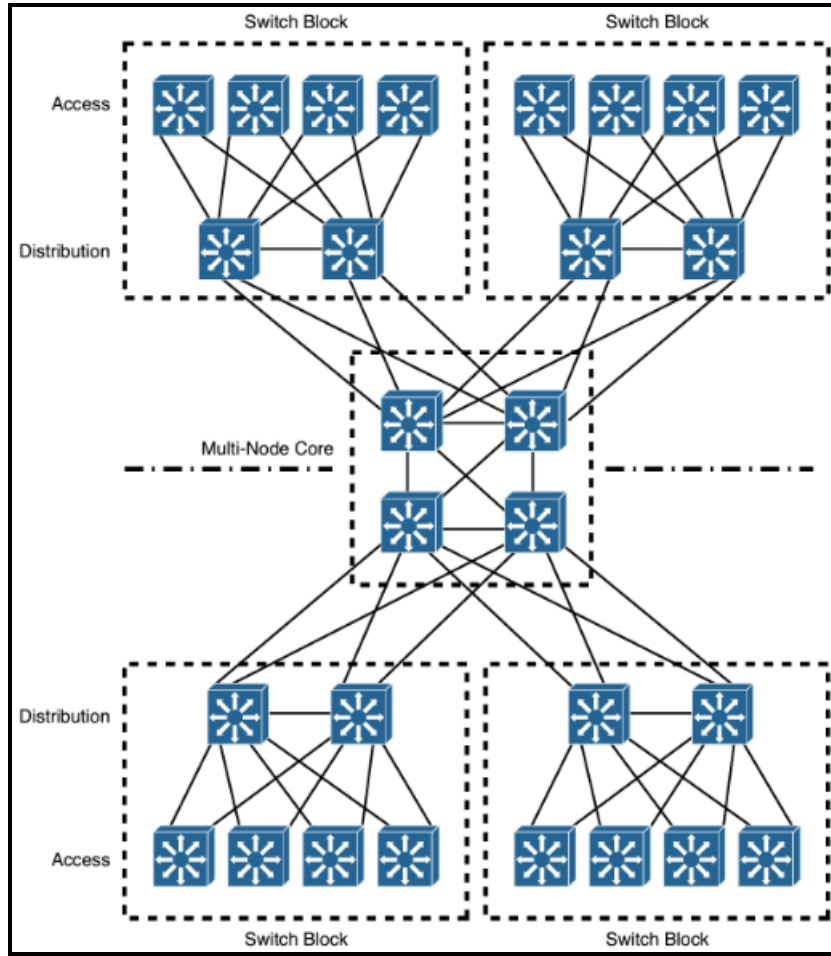


Figure 2: Multinode Core

Multi-Tier Architecture

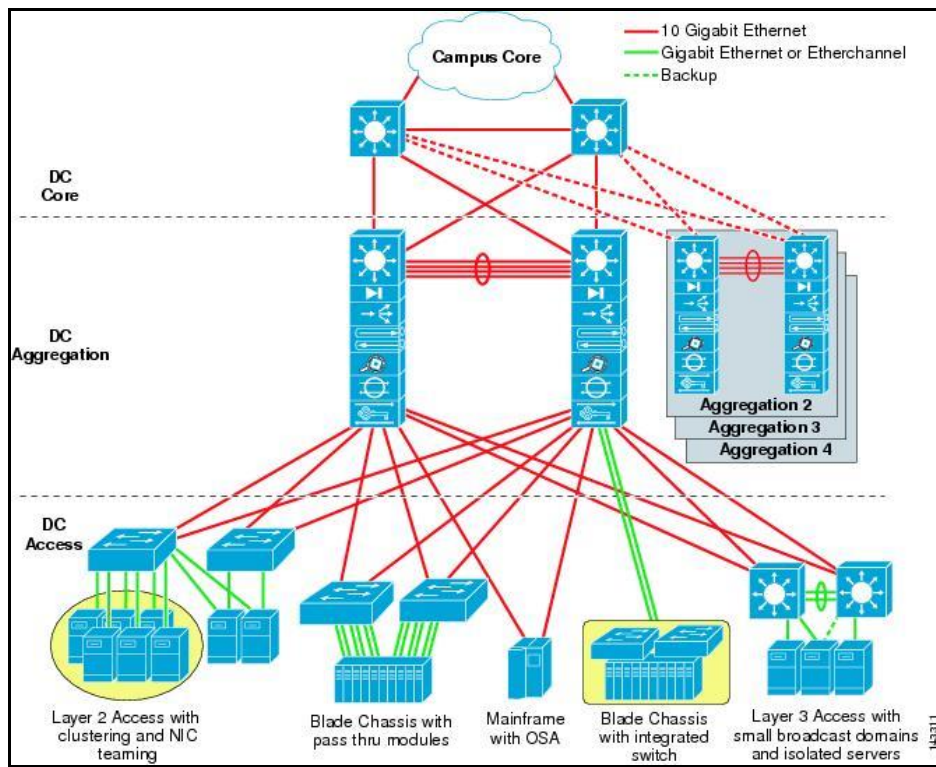


Figure 3: Multi-Tier Architecture

Three-Tier Architecture

- The design uses a partial mesh of links between access and distribution switches
- The design uses a partial mesh of links between the distribution and core switches
- The access layer looks like a star design

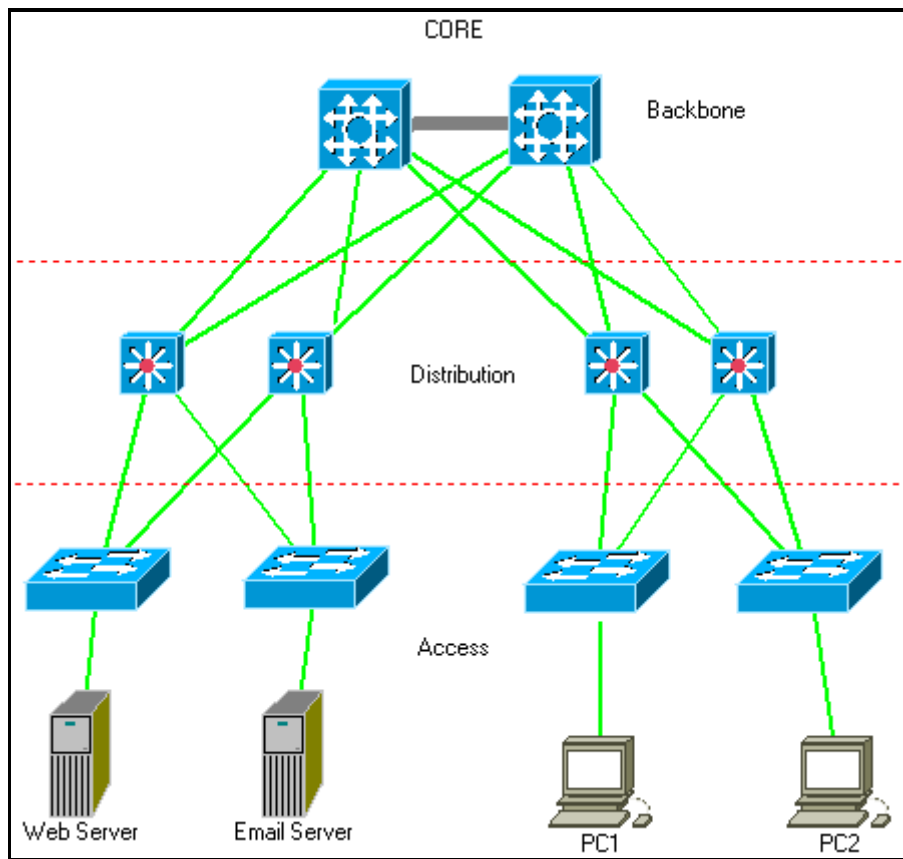


Figure 4: Three-Tier Architecture

Two-Tier Architecture

- The design uses a partial mesh of links between access and distribution switches
- The end user and server devices connect directly to access layer switches

Typical Components of an Enterprise Network

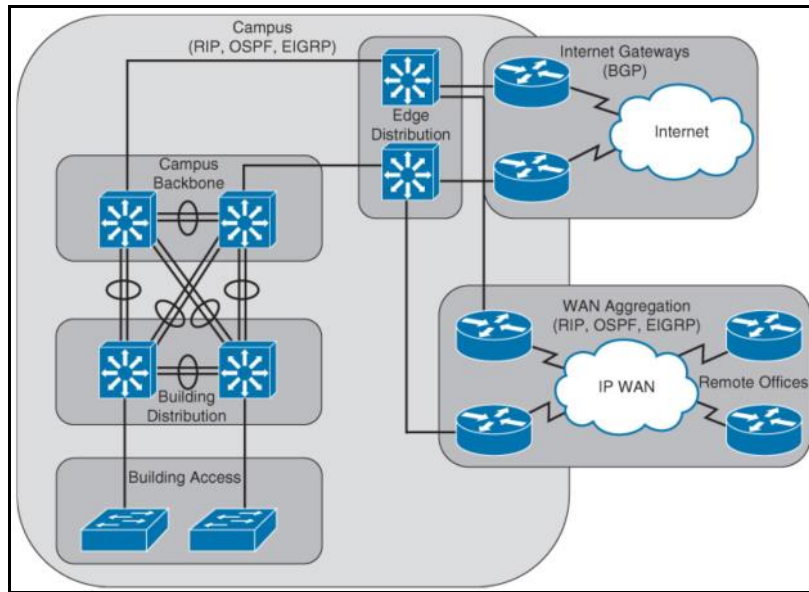


Figure 5: Typical Components of an enterprise Network

- Building Access
- Building Distribution
- Campus Backbone
- Edge Distribution
- @Internet Gateways
- WAN Aggregation

CORE-Layer (Backbone)

- A campus network's core layer provides **connectivity between all distribution layer devices**.
- When the distribution and core layers are combined into a single layer of switches, a **collapsed network** result.
- A core layer is required to **connect two or more switch blocks** in a campus network.
- A core layer consists of **two multilayer switches** that connect two or more **switch blocks** in a redundant fashion.
- A redundant core is sometimes called a **dual core**.

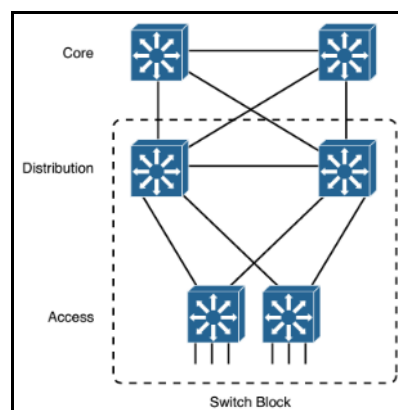


Figure 6: Fully Redundant Hierarchical Network Design

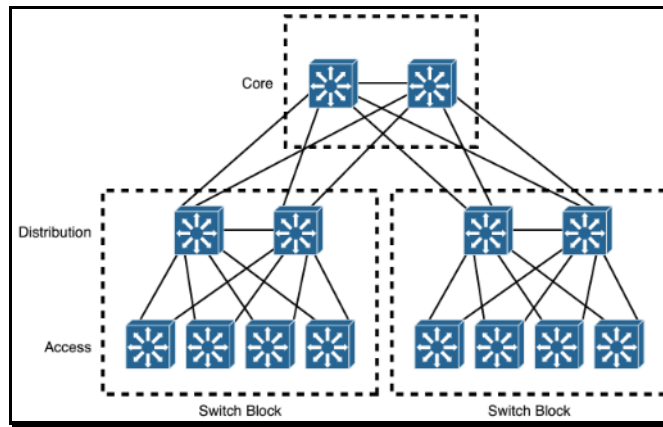


Figure 7: A Redundant Core Layer

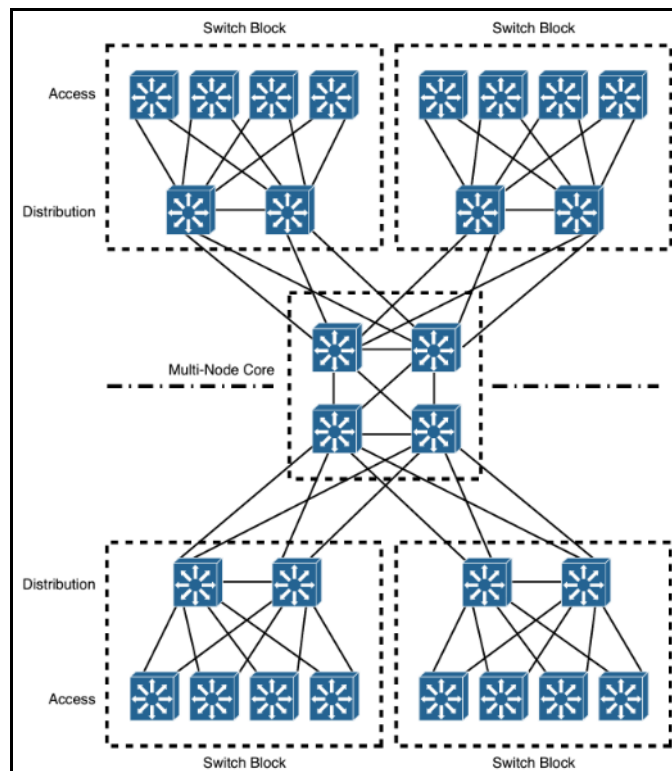


Figure 8: Multi-Node Core in a very large Campus Network

- Each switch block has redundant connections to only one core pair - not to all of the core switches.

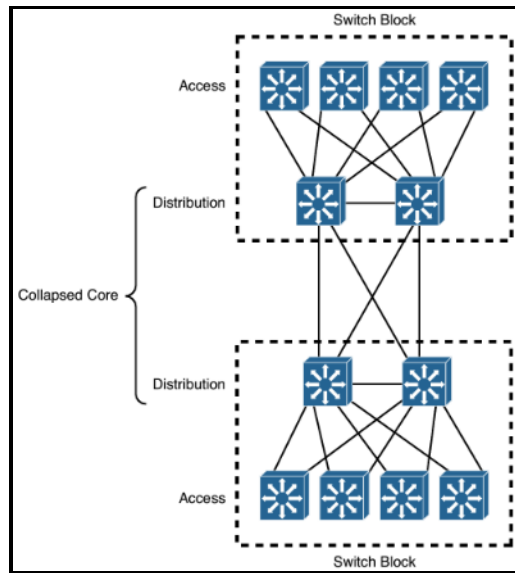


Figure 9: Collapsed Core network design

Distribution-Layer

- The distribution layer provides interconnection between the **campus network's** access and **core layers**.
- In the distribution layer, uplinks from all **access layer devices** are **aggregated**, or come together.
- The distribution layer switches must be capable to **processing the total volume of traffic** from all the connected devices.
- **VLANs** and **broadcast domains** converge at the distribution layer.

Access-Layer

- The access layer exists where the **end users** are connected to the network.
- An access layer incorporates **layer 2 switches** and **access points** granting connectivity between servers and workstations.
- Usually provide **Layer 2 (VLAN)** connectivity between users.

Switch Block

- Designing a switch block based on the number of **users** or **stations** contained within the block is usually inaccurate.
- No more than **2000 users** should be placed within a single switch block.
- A switch block consists of **two distribution switches** that aggregate one or more **access layer switches**.

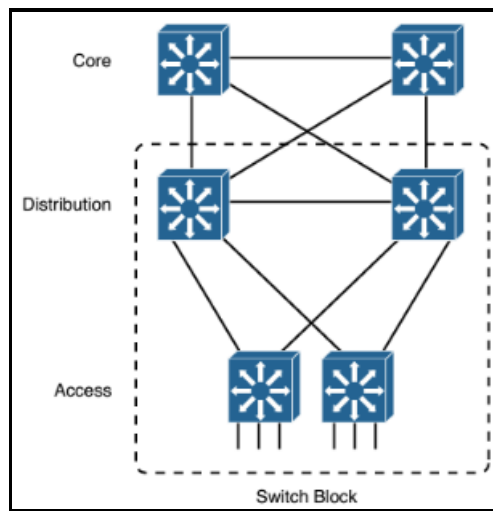


Figure 10: Switch Block

Leaf-Spine Network Topology

- With Leaf-Spine configurations, all devices are exactly the same number of segments away and contain a predictable and consistent amount of delay or latency for traveling information.
- This is possible because of the new topology design that has only two layers, the **Leaf layer** and **Spine layer**.
- The **Leaf layer** consists of **access switches** that connect to devices like servers, firewalls, load balancers, and edge routers.
- The **Spine layer** (made up of switches that perform routing) is the **backbone of the network**, where **every Leaf switch is interconnected with each and every Spine switch**.
- To allow for the predictable distance between devices in this two-layered design, dynamic Layer 3 routing is used to interconnect the layers.
- **Dynamic routing** allows the best path to be determined and adjusted based on responses to network change.
- This type of network is for data center architectures with a focus on “**East-West**” network traffic.
- “East-West” traffic contains data designed to travel inside the data center itself and not outside to a different site or network.
- This new approach is a solution to the intrinsic limitations of **Spanning Tree** with the ability to utilize other networking protocols and methodologies to achieve a dynamic network.

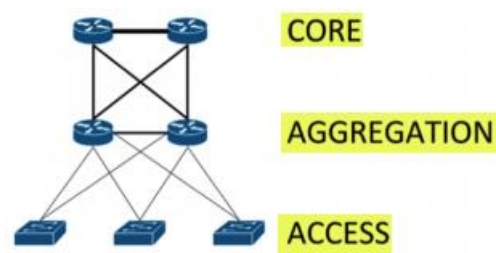


Figure 11: Traditional three-tier network design

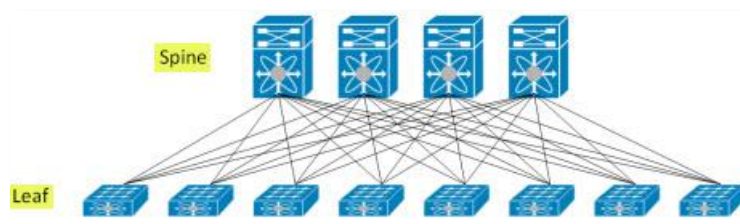


Figure 12: Leaf-Spine architecture design

Routing Protocol Considerations

- Scalability
- Vendor interoperability
- IT staff's familiarity with the protocol
- Speed of convergence
- Capability to perform network summarization
- Interior or exterior routing
- Type of routing protocol

Routing Protocol Migration

Approach 1: Change the **Administrative Distance (AD)** of the new protocol to be higher than the old.
Approach 2: Using **route redistribution**.

IPv6 Migration

- You may use, **Dual-Stack** approach with **NAT64** and or **NPTv6**.
- Or send IPv6 traffic over an **IPv6-over-IPv4 tunnel**.

Network Summarization

- Network summarization allows multiple routes to be summarized in a single route advertisement.
- **OSPF** requires that route summarization be performed only at Area Border Routers (ABR) or Autonomous System Border Routers (ASBR).
- **EIGRP** supports route summarization at any router.
Check in the routing table for summary routes pointing to a **Null interface**.

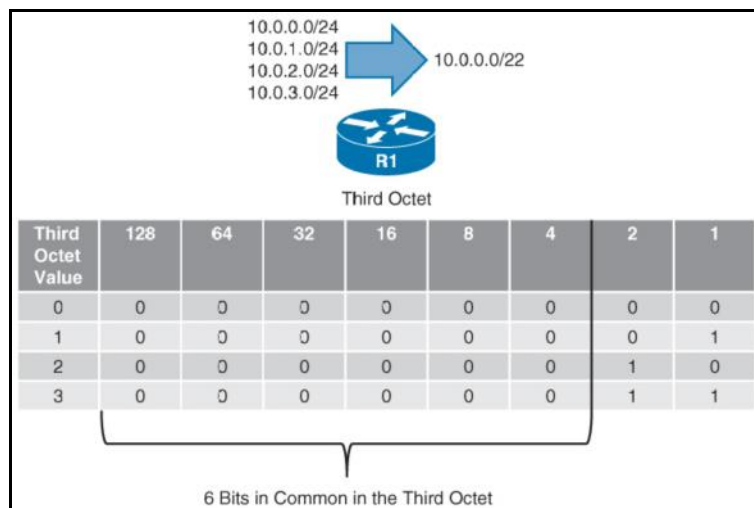


Figure 13: Network Summarization

Network Maintenance Plan

Asynchronous Routing

Also, called **Asymmetric Routing**.

- **uRPF** can be used to avoid asynchronous routing.
- **Conditional advertisement feature** enabled in a multihomed network can be used to prevent asynchronous routes.
- Can be caused by **FHRP** such as **HSRP**, **VRRP**, **GLBP**.
- Can be caused by a **FW**.

Out of order packets

- Can be caused by **Per-Packet load balancing**.

Troubleshooting Models

Simple Troubleshooting Model

1. Problem diagnosis
2. Problem resolution
3. Problem report

Hierarchical Network Design

- ???

Flat Network Topology

- A full Layer 2 only switched network is referred to as flat network topology.
- One **broadcast domain**

OSI-Layers

- *Open System Interconnection*
- ISO 7498
- Logische Struktur für Netzwerkoperationen, standardisiert von der ISO.
- Netzwerkarchitektur mit sieben Schichten zur Definition von Netzwerkprotokollen und Standards.
- Es ermöglicht die Kommunikation zwischen zwei OSI-kompatiblen Computern oder Geräten. Die Schichten lauten:

OSI		TCP/IP	
7	Application Anwendungsebene	GATEWAY	DNS, FTP, NFS, RIP, RLOGIN, SET, SMTP, S-HTTP, POP3, TELNET
6	Presentation Darstellungsebene	Protocol conversion, Encryption/decryption	ASCII, EBCDICM, TIFF, JPEG...
5	Session Sitzungsebene / Steuerungsebene	(e.g. eCommerce Sessions)	NFS, SQL, RPC
4	Transport Transportebene	SPX, NetBEUI, SSL	TCP, ICMP, UDP
3	Network Vermittlungsebene (OSPF, BGP)	XNS, IPX, X.25, CLNP, ES-IS, IS-IS ATM	ROUTER IP, ARP, RARP
		LLC (Logical Link Control)	
2	Data link Sicherungsebene	LAPB/D	BRIDGE LANs, SLIP, PPP, HDLC, CSLIP
		MAC (Media Access Control) (Network Adapter card drivers)	
1	Physical Bitübertragungsebene	REPEATER	HSSI, ISDN, RS-232, RS-499, SDLC, V.34, V.35, X.21, X.24, X.400

OSI Layers		Protocols Mapped to layers	Netware Protocol Stack (Novell)		TCP/IP Protocol Stack			
Application	7	Packet creation, TELNET, Redirector, Electronic message handling, Gateway Protocol conversions	NCP	SAP	FTP	SNMP	Telnet	SMTP
Presentation	6							
Session	5	Synchronization between user tasks by putting checkpoints in the Data stream Performs name recognition and the functions needed to allow two applications to communicate over the network NETBIOS						
Transport	4	NetBEUI, Original Block of Data is broken down into packets	SPX (NWLink)		TCP UDP			
Network	3	X.25, Routers	IPX	RIP	NLSP	IP		
		LLC (Logical Link Control)						
Data Link	2	IEEE 802.2 802.3 802.4 802.5 Bridges	ODI		DATA LINK			
		MAC (Media Access Control) (Network Adapter card drivers)						
Physical	1		Physical		Physical			

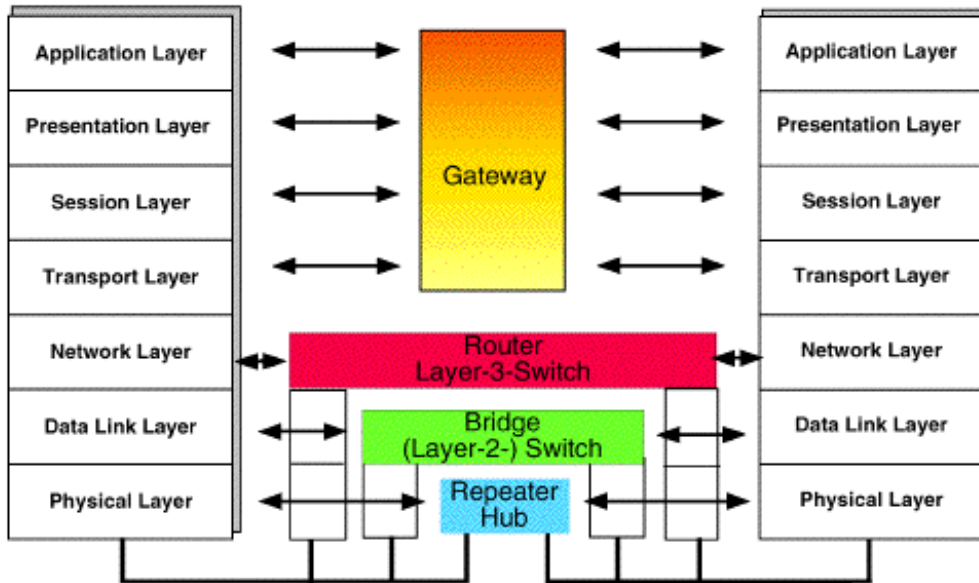


Figure 14: OSI Layers

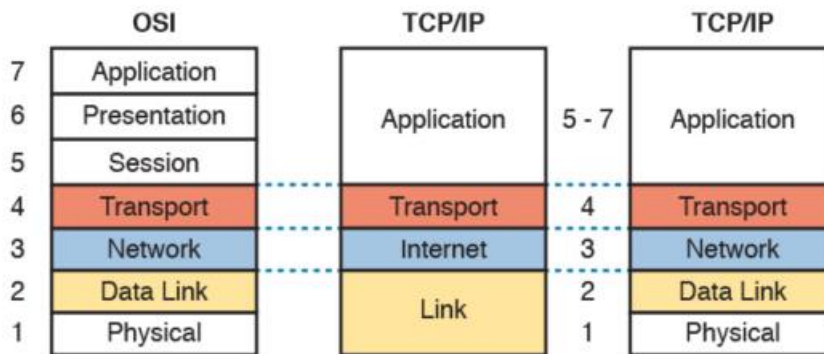


Figure 15: OSI versus TCP/IP

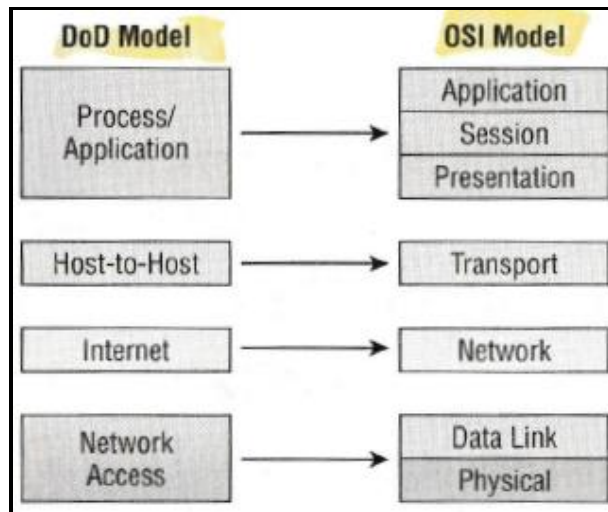
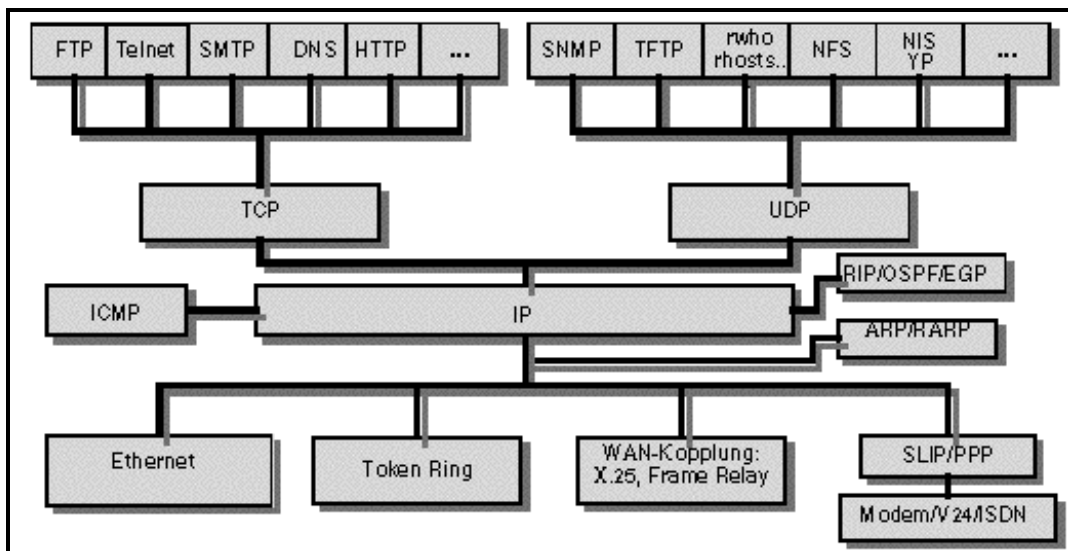


Figure 16: DOD and OSI Model



- UDP = User Datagram Protocol
- CLNP = Connectionless Network Protocol Verzeichnis
- ES-IS = End System to Intermediate System
- FTAM = File Transfer, Access and Management
- IS-IS = Intermediate System to Intermediate System
- LAPB/D = Link Access Protocol

Telnet, FTP und SMTP bauen auf **TCP** auf.
 RIP, DNS, TFTP, NFS, SNMP und Broadcast auf **UDP**.

Physical Layer (Layer 1)

- **Hubs, Repeaters, Concentrators** and **Amplifiers**.
- Defines the physical properties of the network, such as **voltage levels, cable types** and **interface pins**.

Data Link Layer (Layer 2)

- This layer works with **NICs**.
- **ARP** is used to find the way between NICs.

The Data Link Layer contains two sublayers:

- **Logical Link Control (LLC)**
- **MAC sublayer**

Network Layer (Layer 3)

- Is responsible for adding routing and addressing information to the data.
- The network layer is responsible for providing **routing** or **delivery information**, but is not responsible for verifying guaranteed delivery (that is the responsibility of the Transport Layer)

Transport Layer (Layer 4)

- The Transport Layer is responsible for managing the integrity of a connection and controlling the session.
- Session rules specify how much data each segment can contain.
- Ensures **reliable** arrival of messages and provides **error checking** mechanisms and **data flow controls**.

Session Layer (Layer 5)

- The Session Layer is responsible for establishing, maintaining, and terminating **communication sessions** between two computers.

- Communication sessions can operate in one of three different modes:
Simplex
Half-Duplex
Full-Duplex
- **RPC** is implemented on this layer.

Presentation Layer (Layer 6)

- The Presentation Layer is responsible for transforming data received from the Application Layer into a format that any system following the OSI model can understand.
- The Presentation Layer is also responsible for encryption and compression.

Application Layer (Layer 7)

- The Application Layer is responsible for interfacing user applications, network services, or the operating system with the protocol stack.
- **Application Layer FWs** also operate at this layer.
- **Gateways** operate on this layer.

INTERNETWORKING

Network Segmentation

- Breaking up a massive network into several smaller networks with **routers**, **switches** and **bridges**.

Possible causes of LAN Traffic Congestion

- Too many hosts** in a collision or broadcast domain
- Broadcast storms
- Too much multicast traffic
- Low bandwidth
- Adding hubs for connectivity to the network
- A bunch of **ARP broadcasts**

HUB

- HUBs are working on **physical layer** (OSI-Layer 1)
- HUBs don't segment a network
- HUBs are creating **one big collision domain** and **one big broadcast domain**
- If a HUB is attached to a switch, it must operate in **half-duplex** mode because the end stations must be able to detect collision.

Switch

- Switches are working on **data link layer** (OSI-Layer 2)
- There are also **Network Layer 3** switches
- Each port on a switch represents an own **collision domain** within a single **broadcast domain**.
- By default, all switches are configured to be VLAN Trunk Protocol - Servers (**VTP servers**).
- There is **no power button (on/off)** on Cisco switches!
- Supports:
 - **High Port Density**
 - **Large Frame Buffers**
 - **Port Speed**
 - **Fast Internal Switching** up to 10 Gb/s
 - Low Per-Port-Cost

Best Practise: Set the Mode manually

```
(config-if)#duplex auto | full | half
```

Best Practise: Set the Speed manually

```
(config-if)#speed auto | 10 | 100 | 1000 | auto
```

Best Practise: Add Descriptions to the Port

```
(config-if)#description [PC1]
```

Configuring Switch

```
#hostname SW1
```

Management

```
int VLAN1
ip address [IP] [Subnet]
no shutdown
ip default-gateway [IP]
interface [IF]
```

```
description TRUNK
switchport mode trunk
```

```
or
description ACCESS
switchport mode access
```

```
or
```



```
description ROUTED
no switchport
```

Troubleshooting Switch

```
#show version
#show interfaces
#show interfaces status
#show interface trunk
#show interface [IF] switchport
#show interface [IF] status

#show ip interface brief
#show port [IF]

show control-plane host open-ports
show interface switchport brief
show interface switchport module [x]

#show module

#show vlan
```

Bridge

- You would use a bridge in a network to reduce **collision** within **broadcast domains** and to increase the number of **collision domains** in your network.
- **Multiport Bridges** allow only **half-duplex** operation
- Connect unlike media (such as UTP to FDDI) and cabling topologies
- Solve segment bottleneck problems by dividing a busy segment into smaller segments
- Extend a segment and increase the total number of computers on the network
- Similar to Repeaters in the way they join two segments together
- Bridges are not capable of translating or interpreting protocols
- Forwards packets based on the MAC sublayer address
- E.g. **link an Ethernet Segment with a Token Ring segment** and reduce network traffic

Router

- Routers are basically employed to efficiently break up a **broadcast domains** and **collision domains**.
- They don't forward broadcast by default.
- They can **filter** the network based on layer 3 (IP).
- **Back-to-back cable** used for router to router connection (DCE / DTE)
- Use **routing tables** to keep information on the paths to other routers.
- Routers can only route packets **using routable protocols** such as IP, IPX, OSI, DECnet, XNS, and DDP. **Cannot route NetBEUI (non-routable)**
- Can be used to **control broadcast, regulate Traffic** and **provide connectivity in an environment of multiple communication path**.

Router architecture:

- **Management Plane**
The management plane is concerned with the management of the device.
- **Control Plane**
The control plane is concerned with making packet-forwarding decisions.
- **Data Plane**
The data plane is concerned with the forwarding of data through a router.
Forwarding of IP unicast traffic using hardware.

In general, Cisco routers support the following **three primary modes** of packet switching:

- **Process switching**
An interface can be configured for process switching by disabling fast switching on that interface
`no ip route-cache.`

- **Fast switching**
Fast switching is based on the information's stored in the **fast cache**. This can dramatically reduce CPU utilization as compared to **process switching**.
Enable fast switching by using command: `ip route-cache`.
Show the entries with: `show ip cache`.
- **Cisco Express Forwarding (CEF)**
 - Packet switching (via Access lists)
 - Packet filtering
 - Internetwork communication
 - Path selection

When a router routes packets, the router removes the packet's Layer 2 header, examines the Layer 3 addressing and decides how to forward the packet. The Layer 2 header is then rewritten with new source and destination MAC and recalculated CRC.

Configuring Router

```
#ip http secure-port 4433          → The router will listen for HTTPS on port 4433
(config)#ip http server           → Enable HTTP server
(config)#ip http authentication local →
-----
(config)#ip tcp mss 1456
(config)#ip tcp path-mtu-discovery → See PMTUD
```

Troubleshooting Router

```
show memory summary              →
show memory allocating-process table →
```

CEF - Cisco Express Forwarding

- **Layer 3** switching technology.
- CEF separates the **control plane software** from the **data plane hardware**.
- CEF maintains two tables in the **data plane** which are populated by the routing table and the ARP cache.
 - **Forwarding Information Base (FIB)** maintains Layer 3 information's
 - **Adjacency Table** maintains Layer 2 next-hop addresses.
- Entire **data flows** can be forwarded at the data plane.
- CEF is less **CPU-intensive** than fast switching.
- CEF is a prerequisite for **NetFlow**.
- Packets with **IP header options** cannot be CEF switched.
- If the packets **MTU is larger** than the MTU of the output interface cannot be CEF switched.
- Packets that are forwarded to **tunnel interface** cannot be CEF switched.
- **Caches** the **Layer 3 information's** even before the router encounters any data flows.

FIB - Forwarding Information Base

- Essentially this is your **CEF table**, prepopulated with all information needed for actual forwarding to occur, which includes L2 reachability information for the next-hop IP addresses in the RIB.
- The **control plane** builds the FIB table.
- Changes in the **routing table** triggers similar changes in the FIB table.

RIB - Routing Information Base

- Technically, each and every routing protocol has its own **RIB (routing database)** all of which are tied together to make the **Main RIB** or **routing table**.

Adjacency Types

- **Discard Adjacency**
Packets are discarded.
- **Punt Adjacency**
Features that require special handling or features that are not yet supported in conjunction with **CEF** switching paths are forwarded to the next higher switching layer for handling.
- **Glean Adjacency**
When a router is connected directly to several hosts, the FIB table on the router maintains a prefix for the subnet rather than for the individual host prefixes. The subnet prefix points to a glean adjacency. When packets need to be forwarded to a specific host, the adjacency database is gleaned for the specific prefix.
- **Drop Adjacency**
Packets are dropped, but the prefix is checked.
- **Null adjacency**
Packets destined for a Null0 interface are dropped.
This can be used as an effective form of access filtering.
- **Cached Adjacency**
Cached Adjacency is the Acknowledgement update received for the adjacency packet sent.

Configuring CEF

```
(config)#ip cef → To enable CEF globally  
(config-if)#ip route-cache cef → To enable it on an interface, use the command.
```

Disabling CEF globally on the router.

```
(config)#no ip cef
```

Disabling CEF on the IF

```
(config-if)#no ip route-cache cef → Disabling CEF
```

Troubleshooting CEF

```
#show ip cef adjacency serial 4/0/1 10.10.78.69 detail  
#show cef → To view information's about packets forwarded.  
#show ip cache → To view the table.  
#show ip interface [IF] → Shows:  
IP CEF switching is enabled = OK  
IP CEF switching is disabled = NOK
```

Brouter

- A brouter is a combination **bridge-router device**.
- It can use its routing capabilities for one protocol and its bridging capabilities for all other protocols.
- A brouter can route routable protocols and bridge Non-routable protocols. It is a more cost-effective solution for managing internetworks than separate Bridges and routers.
- Can be used to connect a network segment using NetBEUI with another segment using the TCP/IP protocol.
- Function of a Repeater

Repeaters

- Repeaters are devices that can take the weak signal from one network segment and regenerate it.
- A regenerated signal is not just amplified; the original signal is recreated, and then transmitted again at full strength.
- Repeaters can pass data packets from one media type to another media type (e.g. **from coaxial cable to twisted pair**) provided they are using the **same access method** (e.g., Token Ring, Ethernet, or ARCnet).
E.g **Connection of a thinnet coax segment to a thicknet segment**

Token Ring Hub

- 10-port capacity with connections for 8 nodes and ring-in (RI) and ring-out (RO)
- Join up to 33 hubs in one ring
- MSAU networks can have 72 UTP connections and 260 STP connections
- Cable type 1 max. distance from Computer to HUB = 101 feet
- Maximum length between a computer and an MSAU using **Type 1 Cable is 330 feet**
- Cable type UTP max. distance from Computer to HUB = 45 feet
- Cable type STP max. distance from Computer to HUB = 100 feet
- Cable type 6 max. length of patch cable = 150 feet
- IBM Cable Type 3 UTP most frequently used
- Type 3 cable and repeater can extend the distance between **2 MAUs by up to 365 meters.**
- Using appropriate repeaters with type 1 or 2 cable can extend the segment by up to 730 meters.
- Available in 4 Mbps and 16 Mbps.
- Max. distance between MSAU's connected by **Type 3 cable in a Token Ring Network is 1200 feet**
- Distance limitation from one **MSAU to another in a Token Ring network is 500 feet**

Token Ring - Frame Format

Frame Field	Description
Start Delimiter	Marks the start of the frame
Access Control	Identifies the frame as a token or data frame, and the frame priority
Frame Control	Houses either media Access Control (MAC) information for all computers, or „end station“ information for a single computer.
Destination Address	Specifies the target computer MAC address.
Source Address	Specifies the source computers MAC address
Data (Payload)	The information being sent
Frame Check Sequence	Cyclic Redundancy Check information for the frame
End Delimiter	Marks the end of the frame
Frame Status	Marks the frame as being recognized, copied or whether the destination address was available.

IOS License Management

- **Cisco License Manager (CLM)**
- **Ciscos's Product License Registration Portal**
www.cisco.com/go/license
- There was no licensing before **IOS 15.0**
- Temporary licenses expire after **60 days**
- **Right-To-Use (RTU)** licensing
- With IOS 15.0 th package is called **universal image**
- All routers come with the **IP Base licensing (Default)**
 - Data: MPLS, ATM and multiprotocol support
 - Unified Communications: VoIP and IP telephony
 - Security: Cisco IOS Firewall, IPS, IPSec, 3DES and VPN
- To obtain the license you need the **UDI**
Product ID (PID) and the serial number of the router

Install new license file (not PAK):

```
license install [url]
license install flash:[x].lic
```

```
copy tftp flash0
```

Install new Product Activation Key (PAK):

```
license call-home
```

Install right-to-use license

```
license boot module c2900 technology-package [t-package]
```

Backup license

```
license save flash:[x].lic
```

Uninstall license

Disable the technology package.

```
license clear [x]  
no license boot module c2900 technology-package [x] disable
```

Troubleshoot License:

```
show license  
show license udi           → Shows UDI/PID/SN  
show license feature  
show version
```

Cisco Wireless LAN Controllers (WLCs)

- Cisco Unified Wireless Network (**CUWN**) solution.
- **CAPWAP**
- Lightweight Access Point Protocol (**LWAPP**)
DHCP option 43 is used to return the address of the **master controller**.
- Best security with **WPA & 802.1X** authentication.

Cisco 2504	WLC, Small Campus, 1 to 25 Users
Cisco 4400	
Cisco 55xx	WLC, Medium Campus
Cisco 8540	WLC, Large Campus, More than 1000 Users

Wireless Access Point (AP, IEEE 802.11)

IEEE 802.11g → 54 Mbps
IEEE 802.11ac → 2.34 Gbps

Cisco Wireless Access Points

Cisco Aironet 2700 WAP

Same-Layer interaction

- On different computers.
- The two computers use a protocol to communicate with the same layer on another computer.
- The protocol defined by each layer uses a header to communicate.

Adjacent-Layer interaction

- On the same computer.
- On a single computer, one layer provides a service to a higher layer. The software or hardware that implements the higher layer requests that the next lower layer perform the needed function. (Error Recovery)

Bandwidth Delay Product (BDP)

- Refers to the nature of how TCP works and describes **how much data that can be sent in a single TCP stream**.
- The Bandwidth Delay Product is a function of the link **capacity** and **round-trip time**. Because TCP relies on acknowledgements to be sent back by the receiving host for every receive window (which originally had a maximum of 64K) TCP effectively sets a limit on itself.
- In todays, high-speed networks this isn't desirable, so several solutions have been made available, most notably the **Window Size Scaling** and **Selective Acknowledgements**.

Formula: **BDP = total_available_bandwidth (KBytes/sec) x round_trip_time (ms)**

e.g. Bandwidth = 64 Kbps = 8000 Bytes/sec
 RTT = 3 sec
 $8000 \times 3 = 24'000$ Bytes (BDP)

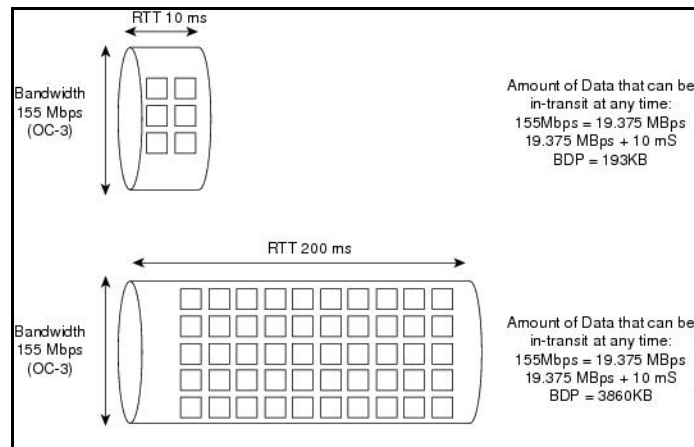


Figure 17: Bandwidth Delay Product (BDP)

Path Maximum Transmission Unit Discovery (PMTUD)

- **TCP MSS** as described earlier takes care of fragmentation at the two endpoints of a TCP connection, but it does not handle the case where there is a smaller MTU link in the middle between these two endpoints.
- PMTUD was developed to avoid fragmentation in the path between the endpoints. It is used to dynamically determine the lowest MTU along the path from a packet's source to its destination.
- If the FW is blocking all ICMP traffic, PMTUD will not work.

Note: PMTUD is only supported by TCP and UDP. Other protocols do not support it. If PMTUD is enabled on a host, and it almost always is, all TCP/IP or UDP packets from the host will have the **DF bit** set.

TCP MSS

- The total data in a **TCP segment**, not including any headers.
- **MSS of 536** is a common value to assure TCP makes it on the way in every possible scenario.

DF-bit Settings:

0	May fragment
1	Do not fragment

Note: **IPv6** does not have a DF-bit.

DSLAM - Digital Subscriber Line Access Multiplexer

- **Layer 2** Device.
- Ist ein Teil der für den Betrieb von DSL benötigten Infrastruktur.
- DSLAMs stehen an einem Ort, an dem Teilnehmeranschlussleitungen zusammenlaufen.
- Meist handelt es sich dabei um eine Vermittlungsstelle, teils aber auch um dezentrale Aufschaltpunkte, z. B. in großen Büro- oder Wohnkomplexen.
- Befindet sich der DSLAM innerhalb der Vermittlungsstelle, spricht man von einem „**Indoor-DSLAM**“, im anderen Fall von einem „**Outdoor-DSLAM**“.

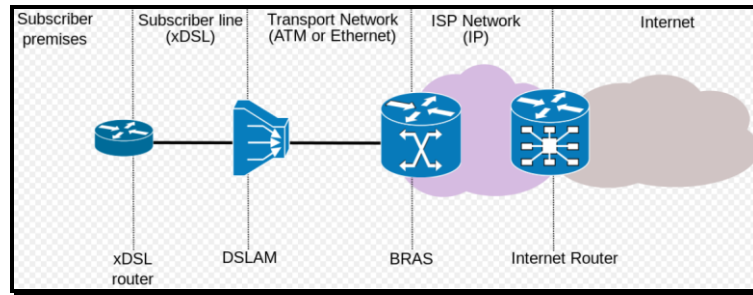
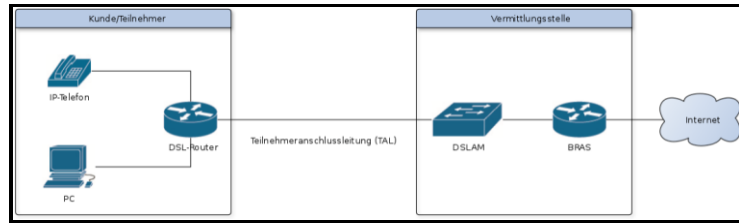


Figure 18: DSLAM



ETHERNET NETWORKS

- Half-Duplex and Full-Duplex.
- Half-Duplex means only one device can transmit at a time.
- CSMA/CD
16 attempts.
Look at the collisions counter.
Look at excessive collisions.
- Interframe gap 9.6 ms ???
- Interframe gap 0.96 ms Fast Ethernet ???
- Collision Detect (CD).
- Max. distance can be 100 m.
- Min. 512 bits.
- Late collision means devices more than 1000m away.
- 802.2, 802.3, SNAP.

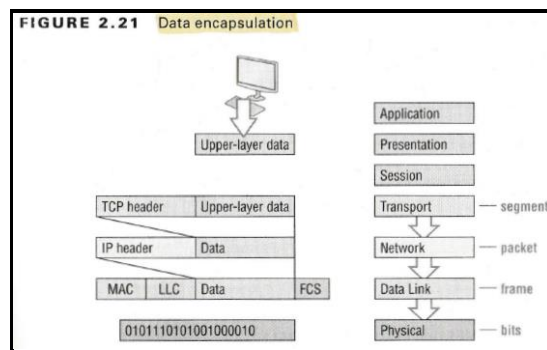


Figure 19: Data Encapsulation

Ethernet uses both:

- Data Link
- Physical Layer

Encapsulation

[Ethernet [IP [TCP [HTTP]]]]]

[Ethernet [IP [TCP [SSL [HTTP]]]]]]

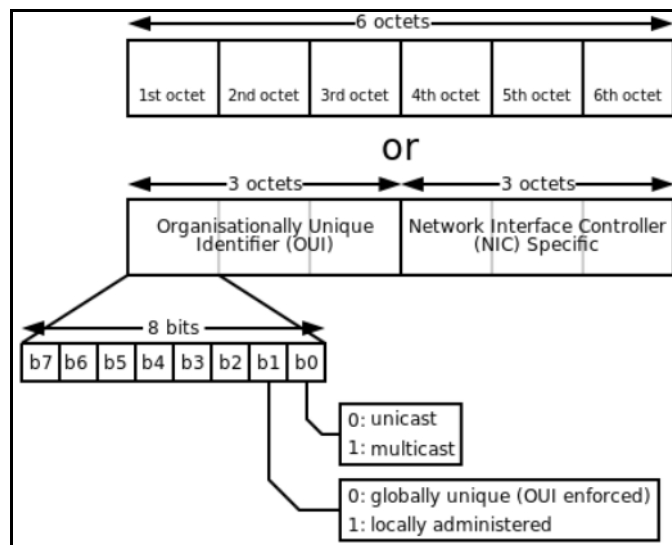
[Ethernet [IPsec [IP [TCP [SSL [HTTP]]]]]]]

Ethernet Type	Media	Maximum Segment Length
10BASE-T	TIA CAT3 or better, 2 pairs	100 m (328 feet)
100BASE-T	TIA CAT5 UTP or better, 2 pairs	100 m (328 feet)
1000BASE-T	TIA CAT5e UTP or better, 4 pairs	100 m (328 feet)
10GBASE-T	TIA CAT6a UTP or better, 4 pairs	100 m (328 feet)
10GBASE-T ¹	TIA CAT6 UTP or better, 4 pairs	38–55 m (127–180 feet)
1000BASE-SX	Multimode fiber	550 m (1800 feet)
1000BASE-LX	Multimode fiber	550 m (1800 feet)
1000BASE-LX	9-micron single-mode fiber	5 km (3.1 miles)

¹ The option for 10GBASE-T with slightly less quality CAT6 cabling, but at shorter distances, is an attempt to support 10Gig Ethernet for some installations with CAT6 installed cabling.

MAC-Address

Win Cmd: `ipconfig /all` or `getmac /v`



in 1st part of Mac address which is **OUI**, the 3rd octet's two Least significant bits are known as **I/G** & **G/L**.

I/G (Individual/Group) bit if set to 0 the communication is Unicast, if bit is set to 1 the communication is broadcast or multicast

Bit 1

0 = I(Individual) / Unicast

1 = G(Group) / Multicast, Broadcast

U/L (Universal/Local)

Bit 2

0 = Universal Administered Address (UAA)

1 = Locally Administered Address (LAA)

OUI - Organizationally Unique Identifier

See: <http://standards.ieee.org/regauth/oui/index>

Extended Unique Identifier

- The IEEE has decided that MAC-48 is an obsolete term and should be depreciated in favor of EUI-48.
- There is also a move to convert from EUI-48 to EUI-64 for future adoption of IPv6.

EUI-48

EUI-64

MAC-Address Table (CAM)

- Content-Addressable Memory (CAM)
- Populated on Bridges and Switches when a Ethernet Frame is received, based on the **source MAC-Address**.
- Switches and Bridges are keeping the MAC-Address by **default 5 min.** in the MAC-Address Table and start a timer (Aging).
- By default, idle CAM table entries are kept for **300 seconds** before they are deleted.
- Only a limited number of **Logical Operation Units (LOUs)** are available in the TCAM.

```
#show mac address-table
#show mac address-table count
#show mac address-table interface [IF]
#show mac address-table aging-time
#show mac address-table dynamic address [MAC]
```

Change the CAM Aging-Time

```
(config)#mac address-table aging-time 600 → Seconds (Default 300)
```

Create a static entry

```
(config)#mac address-table static [MAC] vlan [ID] interface [type]
```

Clear the CAM

```
#clear mac address-table dynamic
```

TCAM

- Ternary Content-Addressable Memory (TCAM)
- There are two components of the TCAM, **Feature Manager (FM)** and **Switching Database Manager (SDM)**.
- The **SDM** manages the **memory partitions** in a switch.
- The TCAM is an extension of the CAM table concept.

```
#show platform tcam utilization
#show sdm prefer
```

Change the SDM template

```
(config)#sdm prefer [template]
```

TCP/IP

- Also called **DARPA** or the **DoD** model, has only **four layers**.
- A **TCP wrapper** is an application that can serve as a basic FW by restricting access to ports and resources based on user IDs or system IDs.
- Using **1236074** is a form of **port-based access controls**.
- **Data flow** is controlled through a mechanism called **sliding windows**.
- TCP/IP is a **multilayer protocol**.

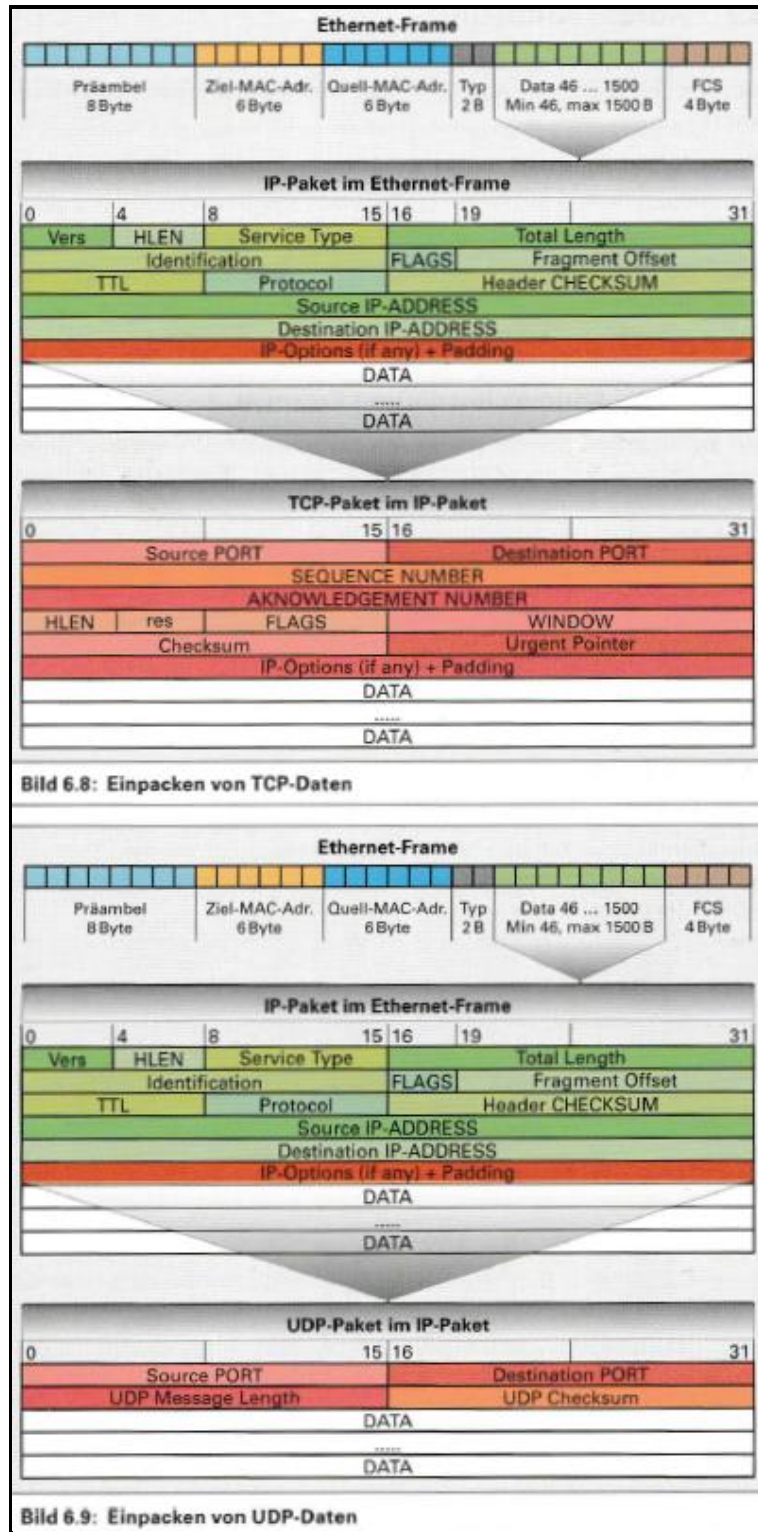


Figure 20: Encapsulate TCP/UDP

IP - Internet Protocol

- IP provides route addressing for data packets.
- IP is connectionless and is an unreliable datagram service.
- IP does not offer guarantees that packet will be delivered or that packets will be delivered in the correct order and it does not guarantee that packets will be delivered only once.

IGMP - Internet Group Management Protocol

RFC 1112

- IP Header 2.
- Allows systems to support multicasting.
- Used by IP hosts to register their dynamic **multicast group membership**.
- Used by **routers** to discover multicast groups.

CIDR - Classless Inter-Domain Routing

See: <http://tools.ietf.org/html/rfc4632>

IPv4

- **IPv4 fragmentation** makes it difficult for a firewall to filter fragmented packets.
- **4 Byte** long address

Classful Network Concept

Reserved	0.0.0.0/8	Used for self-identification on a local subnet
A-Class	1.0.0.0 - 126.0.0.0 Octet 1-126	16'777'216 Addresses/Network
Reserved	127.0.0.0/8	Loopback testing
B-Class	128.0.0.0 - 191.255.0.0 Octet 128-191	1'048'576 Addresses/Network
Reserved	169.254.0.0/16	APIPA
Reserved	192.0.2.0/24	For use in documentation and example code
Reserved	192.88.99.0/24	Used for IPv6-to-IPv4 relay (RFC 3068)
C-Class	192.168.0.0 - 192.168.255.255 Octet 192-223	65'536 Addresses/Network IP address starts with: 110....
Reserved	198.18.0.0/15	Benchmark testing for @Internet devices (RFC 2544)
D-Class	Multicast Addresses Octet 224-239	
E-Class	Experimental Octet 240-255	

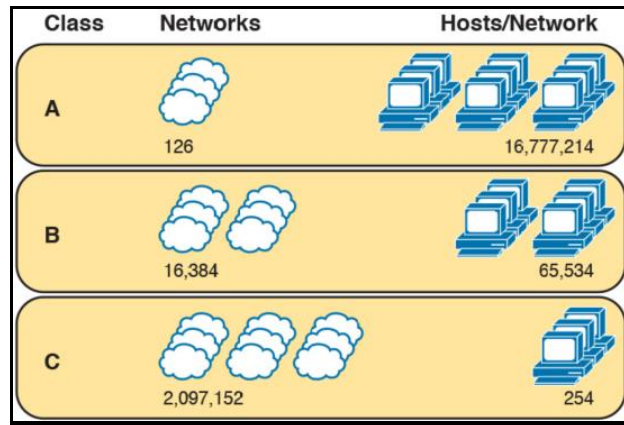


Figure 21: Numbers and Sizes of Class A, B and C Networks

Private IPv4 Address Spaces

A-Class	10.0.0.0 - 10.255.255.255	16'777'216	Addresses
	10.0.0.0/8		
	Octet 1-126		
	Valid networks 1.0.0.0 - 126.0.0.0		
B-Class	172.16.0.0 - 172.31.255.255	1'048'576	Addresses
	172.16.0.0/12		
	Octet 128-191		
	Valid networks 128.0.0.0 - 191.255.0.0		
C-Class	192.168.0.0 - 192.168.255.255	65'536	Addresses
	192.168.0.0/16		
	Octet 192-223		
	Valid networks 192.0.0.0 - 223.255.255.0		

IPv4 Multicast Addresses

Link: <http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml>

- A **single device** is sending traffic to a predefined **group of receivers**.

222.0.0.0 - 224.0.1.255	Permanent Multicast Groups
232.0.0.0 - 232.255.255.25	Source-Specific Multicast (SSM)
233.0.0.0 - 239.255.255.255	GLOP Addresses
239.0.0.0 - 239.255.255.255	Private Multicast Addresses

Class **D** Network is used for Multicast addresses (1110).

224.0.0.1	All multicast hosts
224.0.0.2	HSRP/ Route messages to all multicast routers
224.0.0.4	DVMRP routers
224.0.0.5	OSPF SPF routers
224.0.0.6	OSPF DR routers
224.0.0.9	RIPv2 routers
224.0.0.10	EIGRP routers
224.0.0.13	PIM routers
224.0.0.18	VRRP advertisements
224.0.0.22	IGMPv3
224.0.0.25	RGMP
224.0.0.102	GLBP (UDP port 3222)
224.0.1.39	Cisco-RP-Announce
224.0.1.40	Cisco-RP-Discovery
224.0.1.60	HP-Device-Disc
239.255.255.250	UPnP (SSDP)

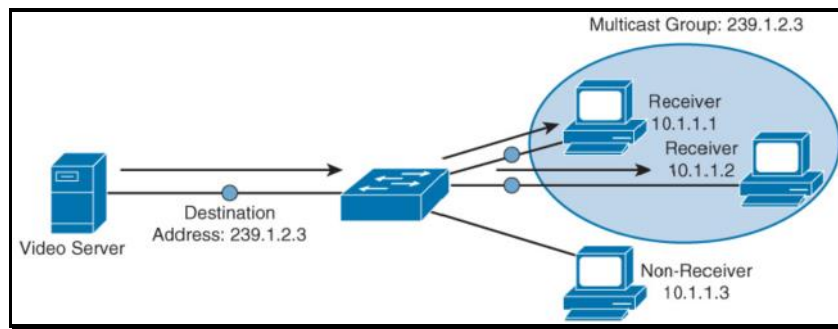


Figure 22: Multicast Traffic

APIPA - Automatic Private IP Addressing

RFC 3927

- Aka **link-local address** assignment.
- Primarily a feature of **Windows**.

Range:

169.254.0.1 - 169.254.255.254 (255.255.0.0)

Unicast

- Traffic travels from a **single source** device to a **single destination** device.

Unicast Flooding

- The very cause of unicast flooding is that destination MAC address of the packet is not in the L2 forwarding table of the switch. In this case, the packet will be flooded out of all forwarding ports in its VLAN (except the port it was received on).
- May lead to partial or complete connectivity interruption between hosts on a network.

Causes:

1. Asymmetric Routing
2. Spanning-Tree Protocol Topology Changes
3. Forwarding Table Overflow

Broadcast

- Broadcast traffic travels from a **single source** to all destinations in a **subnet** (Broadcast-Domain).
- **Layer 2 Broadcast**
Hardware Broadcast they only go out on a LAN.
- **Layer 3 broadcast**
Reaches all hosts on a broadcast domain.
- **Subnet Broadcast**
Also called the subnet broadcast address or directed broadcast address or all-host broadcast, this is the last (numerically highest) number in the subnet.
Directs all devices in a remote network.
- **Network Broadcast address**
One reserved address for each classful network, namely the numerically highest number in the network. Used to send one packet to all hosts in that network. Also called an all-subnets broadcast, referring to the fact that the packet reaches all subnets in a network.

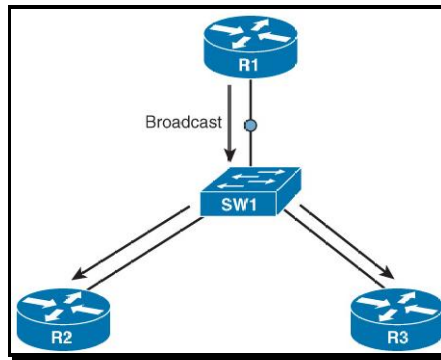


Figure 23: Broadcast Network Type

Interface Naming Conventions

E0	EtherFast Interface
Fe0/0	Fast Ethernet (10/100)
Ge0/0.1	Gigabit Ethernet / One physical interface with multiple sub interfaces
Lo0	Loopback Interface
OOB	Out-of-Band Port
S0/0	Serial Interface
XGe1/1/1	Ten Gigabit Ethernet ports (1000/10,000 Mbps)

Global Synchronization / TCP Synchronization

- If a router interface drops simultaneously **TCP flows (TCP slow start)**, this is called **global synchronization**.
- To prevent **global synchronization**, Cisco IOS supports a feature called **Weighted Random Early Detection (WRED)**.

End-to-End Delay

- Equals the **sum** of all propagation, processing, serialization and queueing delays in a network path.

Troubleshooting: Latency/Packet-Loss

General information needed for troubleshooting "Latency/Packet-Loss" problems:

Define concerned device <	>	e.g. me-sgxxx...	LIT
Check the ISPs in OS/MC:			
- ISP1		OK/NOK	LIT
- ISP2		OK/NOK	LIT

Troubleshooting: TCP/IP

General information needed for troubleshooting network related problems:

Minimum Informations (Mandatory)

IPCONFIG /ALL
NSLOOKUP <Destination-System>
PING 127.0.0.1 | LOCALHOST
PING <Own IP>
PING <Default Gateway IP> | <Default Gateway Name>
PING <Remote-Host>
PATHPING <host>

IPv6

PING ::1
PING <FE80...>
PING 2001:....
TRACERT / TRACEROUTE <2001....>

Extended Informations

TRACERT / TRACEROUTE <Destination-System>
ROUTE PRINT
ARP -a Displays content of ARP cache
show ip arp Cisco: View contents of the ARP Cache

Special informations (FW-Related):

NETSTAT -an (Admin rights necessary)

SC QUERY > temp.bat (Send file <temp.bat>)

Network Related Registry

<ncpa.cpl> or <control netconnections>
gpresult /R
msinfo32
SC query

MTU + RWIN für DSL
Xxxxx

@Internet increase amount of connections:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings <MaxConnectionsPerServer>

Antwortzeit(Timeout) von Webseiten erhöhen:
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings <KeepAliveTimeout>

Netzwerkordner erst beim Zugriff prüfen:
HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider <RestoreConnection>

Cache für NT File System vergrößern
HKLM\SYSTEM\CurrentControlSet\Control\FileSystem <NtfsMftZoneReservation>

Wartezeit hängende Applikation (HungAppTimeout)
Xxxx

Wartezeit hängende Applikation (WaitToKillAppTimeout)
Xxxx

Windows Firewall Konfigurieren
Log befindet sich unter <C:\WINDOWS\pfirewall.log>

PING Round-Trip-Time (RTT) shows the time it takes for a signal to be sent, plus the length of the time it takes for an acknowledgement of the signal to be received.

Examples:

ping loopback	Test local config
ping localhost	Test local config
ping 127.0.0.1	Test local config
ping <hostname>	Test reachability
ping <IP-Address>	Test reachability

ping <IP > -t -l 65500	Max. Stress test 1 (MTU)
ping <IP > -t -a -f -l 1450	Max. Stress test 2 (MTU)
Msg: Packet needs to be fragmented but DF is set to 1.	
ping -L	Larger size packets

Ping return codes by Cisco IOS

- !** Indicates that the ICMP echo reply was received and that the ping was successful.
- .** Indicates that the ICMP echo reply was not received.
 - A firewall or an access list has blocked the ping request.
 - A router in the path did not have a route available for the destination and the router did not respond back with an ICMP destination unreachable message.
 - There was a physical connectivity problem along the path.
- U** Indicates that a router in the path has sent an ICMP destination unreachable message because the router did not have a route available to the destination.
- C** Indicates that a device in the path was receiving a lot of traffic or was congested.
- &** Indicates that a routing loop may have occurred. The packet time-to-live was exceeded.
- M** Indicates a fragment error. The packet needed to be fragmented but it could not be.
- ?** Indicates an unknown packet type.

Public IPs to Ping/Tracert: **8.8.8.8** Google-DNS

Tools: [PingPlotter](#)

ARP Shows locally resolved IP-Addresses as physical addresses

IP- Addressee → MAC- Address

ARP-Type can have one of the following values:

- Static, Dynamic, Invalid, Other.

Examples:

arp	
arp -a	Show ARP Cache
arp -d	Deletes arp-cache

IPCONFIG Shows the actual TCP/IP configuration.

e.g. ipconfig /all

NETSTAT Shows TCP/IP-Protokollstatistics and connections.

This is usefull to research FW related port issues.

Examples:

netstat	Shows connections
netstat -a	Active connections
netstat -an	Active connections
netstat -s	Shows statistics

ROUTE Shows the local routing table.

e.g. route print

HOSTNAME Shows the name of the local host where the command is executed.

TRACERT Traces the route to a remote device.

NSLOOKUP Main diagnostic tool for DNS-Service.

Examples:

```
nslookup
set d2
www.<name>.com
```

FINGER

Frequent Asked Questions (FAQ)

TRACERT to a certain destination doesn't work from a certain PC.

Check your default gateway on the concerned PC.

If default gateway is: 0.0.0.0, you may have an issue with **IPv6-Setup** and/or the **"Bonjour-Service" from Apple**.

Default Gateway become "ON-LINK"

If route print shows something like:

Network	netmask	gateway	
0.0.0.0	255.255.255.0	ON-LINK	
0.0.0.0	255.255.255.0	<x.x.x.x>	→ Your default gateway!

Connection doesn't work because the gateway ON-LINK comes first, all the packages are routed to the gateway ON-LINK where the correct gateway should be <x.x.x.x>.

Maybe that route is added by some applications. You may use the following command to delete this route.

```
route delete 0.0.0.0
```

Tools: MAC Address Identifier

http://www.coffer.com/mac_find

EASY SUBNETTING

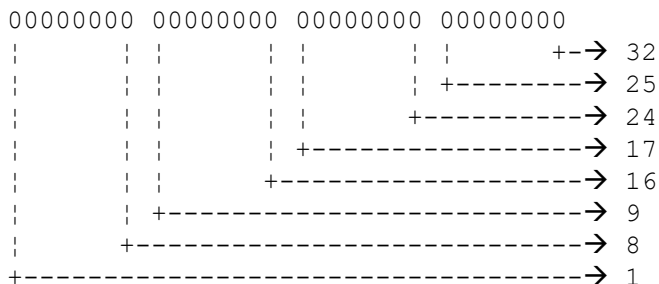
Benefits of subnetting:

- Reduced network traffic
- Optimized network performance
- Simplified management
- Facilitated spanning of large geographical distances

Subnet/CIDR/4TH Octet

Tool: [Subnet Calculator](#)

- **CIDR** defines a way to assign public IP addresses, worldwide, to allow **route aggregation** or **route summarization**. These route summaries greatly reduce the size of routing tables in @Internet routers.



Bits	Mask	S-Bits	H-Bits	S-Block	Tot-Hosts $2^{H-Bits} - 2$	Subnets 2^{S-Bits}	Wildcard S-Block - 1
/32	255.255.255.255	8	0	0	0	256	0.0.0.0
/31	255.255.255.254	7	1	2	0	128	0.0.0.1
/30	255.255.255.252	6	2	4	2	64	0.0.0.3
/29	255.255.255.248	5	3	8	6	32	0.0.0.7
/28	255.255.255.240	4	4	16	14	16	0.0.0.15
/27	255.255.255.224	3	5	32	30	8	0.0.0.31
/26	255.255.255.192	2	6	64	62	4	0.0.0.63
/25	255.255.255.128	1	7	128	126	2	0.0.0.127
/24	255.255.255.0	8	8	256	254	256	0.0.0.255
/23	255.255.254.0	7	9	2	510	128	0.0.1.255
/22	255.255.252.0	6	10	4	1'022	64	0.0.3.255
/21	255.255.248.0	5	11	8	2'046	32	0.0.7.255
/20	255.255.240.0	4	12	16	4'094	16	0.0.15.255
/19	255.255.224.0	3	13	32	8'190	8	0.0.31.255
/18	255.255.192.0	2	14	64	16'382	4	0.0.63.255
/17	255.255.128.0	1	15	128	32'766	2	0.0.127.255
/16	255.255.0.0	8	16	256	65'534	256	0.0.255.255
/15	255.254.0.0	7	17	2	131'070	128	0.1.255.255
/14	255.252.0.0	6	18	4	262'142	64	0.3.255.255
/13	255.248.0.0	5	19	8	524'286	32	0.7.255.255
/12	255.240.0.0	4	20	16	1'048'574	16	0.15.255.255
/11	255.224.0.0	3	21	32	2'097'150	8	0.31.255.255
/10	255.192.0.0	2	22	64	4'194'304	4	0.63.255.255
/9	255.128.0.0	1	23	128	8'388'606	2	0.127.255.255
/8	255.0.0.0	8	24	256	16'777'214	256	0.255.255.255

S-Bits = Subnet-Bits

H-Bits = Host Bits

S-Block = Subnet Range

Nibble Values

8 4 2 1

Byte Values

128 64 32 16 8 4 2 1

Subnet-Zero

Let's consider this class A network, with a custom mask: **50.0.0.0/10**

Possible subnets are:

50.0000 0000.x.x (first subnet, all zeros)
50.0100 0000.x.x
50.1000 0000.x.x
50.1100 0000.x.x (last subnet, all 1s)

A long time ago, it was not allowed to use the all 00 (the first subnet above, also called "subnet zero") subnet, as the subnet bits were all zeros. In that same thinking, it was not allowed to assign (or use) a subnet where all the subnet bits were all 1's, such as the last subnet above.

This limitation can be overruled by the command: **ip subnet-zero**

- ip subnet-zero does not prevent the router to learn subnet-zero nets to learn via routing protocols!

Supernet

- It's the opposite of subnet.

Example: You have 4 Class C Networks:

192.168.0.0/24
192.168.1.0/24
192.168.2.0/24
192.168.3.0/24

and you would merge it to one supernet, then it would like so:
192.168.0.0/22 → supernet

VARIABLE LENGTH SUBNET MASK (VLSM)

VLSM enable the creation of subnets of specific sizes and allow the division of a classless network into smaller networks that do not need to be equal in size. This makes use of the address space more efficient because many times IP addresses are wasted with classful subnetting.

The four CISCO troubleshooting steps:

1. Ping the loopback address
ping 127.0.0.1 → Test your local IP stack
2. Ping the NIC
3. Ping the default gateway
4. Ping the remote device

INTERNETWORKING OPERATING SYSTEM (IOS)

- **Privilege levels** let you define what commands users can issue after they have logged in to a network device.

The IOS File System

- As for the physical storage, Cisco routers typically use **flash memory**, with **no hard disk drive**, because there are no moving parts in flash memory, so there is a **smaller chance of failure**.
- IOS file system (IFS)

<code>show file systems</code>	→ Shows the IFS
<code>more flash0:/wotemp/fred</code>	→ Displays file fred
<code>dir flash0:</code>	→
<code>verify /md5 [file]</code>	→ Generates the MD5 hash

Router Boot Sequence

1. **POST**
Verifies that all components are working properly
2. Flash Memory (Cisco IOS)
3. NVRAM (startup-config)
4. Setup mode: If no startup configuration is available

Router Modes

- **ROM monitor mode (ROMmon)**
`rommon>`
- **User EXEC mode (Log in / Privilege level 1)**
`router>`
`[no] login`
- **Privileged EXEC mode (Privilege level 15)**
`router#`
`enable` → To enter from User EXEC mode
- **Global configuration mode**
`router(config)#`
`configure terminal`
- **Interface configuration mode**
`router(config-if)#`
`interface`
- **Interface configuration mode range**
`router(config-if-range)#`
- **Interface configuration mode**
`router(config-subif)#`
`interface`
- **Router configuration mode**
`router(config-router)#`
`router ospf [x]`
`router-id 1.1.1.1`
- **VLAN configuration mode**
`router(config-vlan)#`
`vlan [x]`

Hostnames

```
(config)#hostname RTR_1
```

Banners

```
(config)#banner motd # [message of the day] #
(config)#banner exec # [Displayed when a EXEC process is created] #
(config)#banner login # [Displayed before username and password] #
(config)#banner slip-ppp # [Displayed before username and password] #
(config)#banner incoming # [Incoming connection to the terminal line] #
```

```
Router#show ?
access-lists      List access lists
cdp               CDP information
clock             Display the system clock
flash:            display information about flash: file system
frame-relay       Frame-Relay information
history           Display the session command history
hosts             IP domain-name, lookup style, nameservers, and host table
interfaces        Interface status and configuration
ip               IP information
ipv6              IPv6 information
running-config    Current operating configuration
sessions          Information about Telnet connections
spanning-tree     Spanning tree topology
startup-config    Contents of startup configuration
terminal          Display terminal configuration parameters
users             Display information about terminal lines
version           System hardware and software status
```

Figure 24: Privileged Exec mode commands

Setting Passwords

- Password protection lets you restrict access to a **network** or a **network device**.

Setting the router password is **one of the most important configurations!**

Password Types:

Type-0 No encryption
Type-4 SHA-256 Hash
Type-5 MD5 Hash
Type-7 Vigenere Cipher

- ❑ Configure a secure **user account** to make the Router/Switch network security compliant.

```
(config)#service password-encryption
username [user] password [pwd]
or
username [user] privilege [1/7/15] secret [pwd]
```

- ❑ There are **five passwords** you'll need to secure your Cisco routers:

- **console**

```
(config)#line console 0
(config)#password [pwd]
```

```
login [local]
exec-timeout 0 0
```

→ Default 10 Minutes.

- **auxiliary**

```
(config)#line auxiliary 0
(config)#password [pwd]
login
```

- **telnet (VTY)**

```
(config)#username [x] password [y] → User authentication
(config)#ip domain-name [domain]
(config)#crypto key generate rsa → Creates and stores keys in flash
(config)#ip ssh version 2
(config)#line vty 0 4
(config)#password [pwd]
(config-line)#login [local] → Remote user to provide a password
(config-line)#transport input ssh
```

Apply access-list to vty:
access-class access-list [x] in

- (config)#**[no] enable password [level]**
Sets a local password to control access to various privilege levels.
You can specify up to 16 privilege levels, using numbers 0 through 15 (Default).

Use **enable secret** for additional layer of better security.
Check: **show privilege** or **show running-config**

- **[no] enable secret**
Specifies an additional layer of security **over the enable password** command.
Uses **MD5** algorithm, which is less secure than SHA-256.
enable secret [pwd]

Encrypt all the passwords in the configuration file

- (config)#**service password-encryption** → Encrypt passwords
enable secret [5] <removed> →

Password Recovery/Reset

Start in mode **ignore configuration bit**. The second bit in the third nibble, reading left to right. When set to binary 1, the router will ignore the startup-config file the next time the router is loaded.

1. **Change to ROMmon mode**

Older router require to press the break key at the console during start.
On newer routers you may remove the flash memory start the router and put the flash memory back after ROMmon is loaded.

2. rommon 1>**confreg 0x2142**
3. **Reboot** the router with an IOS (flash)
4. Answer the question of **initial configuration** with **[no]**
5. Go into **privileged mode** (enable)
6. **#copy startup-config running-config**
7. (config)#**enable secret [new password]**
8. (config)#**config-reg 0x2102**
9. **#copy running-config startup-config**

Troubleshoot running-config

- service password-encryption
- enable secret 5 <removed>
- enable password [pwd]** → Should no longer be used
- ip domain-name [domain]
- username [user] privilege 1 password 7 <removed>
- line con 0 → Password protection
- line aux 0 → Password protection
- line vty 0 x → Password protection and SSHv2
- shutdown unused network connections
- Configure switchport-security
- show port security interface fax/x
- Is **SCP** enabled
(config)#**ip scp server enable** → Check running-config
Use SCP client to make a backup.

Using the Pipe command

#**show running-config** | ? → Shows help to:
append
begin
exclude
include
redirect
section
tee

#**show running-config** | **begin interface**

```
#show running-config | include frame-relay map
#show running-config | section eigrp
#show running-config | section router
```

```
#show ip route | include 192.168.3.32
#show interfaces | begin Serial
```

```
#show mac address-table | include [mac]
```

Serial Interface Commands

Usually they are connected to a **CSU/DSU** type of device.

Configuring SSH

- To create a RSA key pair, the Host Name and the Domain Name will be used.

```
hostname [SSH_Router]
ip domain-name [domain_name]
username [user] privilege 15 secret [pwd]
crypto key generate rsa modulus [260-4096]
transport input ssh
login local
```

→ Tells the router, to use the local user database for authentication.

```
access-class [acl] in → Optional
```

Configuring SSH for VTY Access

```
hostname [SSH_Router]
ip domain-name [domain_name]
username [user] privilege 15 secret [pwd]
crypto key generate rsa modulus [260-4096]
access-list 1 permit [IP] [WC]
access-list 1 deny any log
```

```
line vty 0 15
access-class 1 in
transport input ssh
login local
```

→ Tells the router, to use the local user database for authentication.

Troubleshooting Interfaces

- **CRC and input errors output grow**
Indication for interference on the Ethernet cable or Cable damage
- **High number of collisions**
Are indicating duplex mismatch
- **Excessive late collisions**
Are indicating duplex mismatch.
They appear after the first 512 bits of data are transmitted.
- **Interface resets are indicating**
Keepalive has been missed, link congestion or hardware issue

Troubleshooting Serial Lines

See: <http://www.cisco.com/en/US/docs/internetworking/troubleshooting/guide/tr1915.html#wp1020941>

```
show interfaces serial [x]
• Lines status
• Output Drops
  No buffer space
  show buffers
```


- Input Drops
Input rate exceeds the capacity of the router
- CRC Errors
- Input Errors
- Carrier transitions
- Framing Errors
- Interface resets
- Abort Errors

debug

ping

Clocking problems

Adjusting Buffers

Serial Line Tests

```
show int [s0/0]
```

```
show controller [t1]
```

- T1 Problems

```
show [e1] controller
```

- E1 Problems

ROUTER SECURITY CONCEPTS

- Cisco term *Defense-in-Depth*.

Router Security Policy

Passwords

- Will passwords appear encrypted in the routers running configuration?
- How often should the passwords be changed?
- How complex should the password be?
- Ideally, all passwords associated with your router would be stored on an external AAA server.
- It's best-practice to encrypt any password appearing in a router' configuration.
- Use `enable secret [password]`.
- Encrypt the line passwords (*VTTY*, *router console* and *auxiliary line*) with `service password-encryption`.
- Use *username* and *password* to login to a router, and not only a password.
`username [user] privilege [0-15] secret [pwd]`.

Authentication

- Will users be authenticated by the routers local database or by an external authentication system such as TACACS+ or RADIUS server?
- Will a AAA server be used to log login/logout events?
- Will a banner be presented to someone logging in?

Access

- What protocols for remote access are allowed (SSH, HTTPS, Telnet, HTTP)?
- If SMTP is configured to use community strings for authentication, how often should those community strings be changed?

Services

- What services should run on the router?

Filtering

- Are private IP addresses (RFC 1918) being filtered?
- How does the router defend against IP spoofing attacks (ACLs and uRPF)?

Routing Protocols

- What kind of authentication is used by the router's routing protocols?

Backups

- How is the router configuration backed up (TFTP server or ...)?
- How often will the router's configuration be backed up?

Documentation

- Define the process, to assure, that all router configuration changes are documented.

Redundancy

- If the router fails, is there a backup router to take over?
- Is the backup router a hot standby router (e.g. HSRP) or is it a cold standby router?

Monitoring

- What parameters are being monitored and logged
CPU utilization, Memory utilization, failed access attempts

Tools:

- **Icinga**: System- und Netzwerküberwachung
- **Nagios**:
- **WhatsUp**
- **Observium**
- **PRTG**

Updates

- What procedure is in place to determine whether security vulnerabilities have been identified?
- What procedure is in place to update the version of Cisco IOS?

RBAC - Role-Based Access Control

- See Security CISSP.docx

Routing Protocol Authentication

- Dynamic routing protocols like **OSPF** and **EIGRP** can dynamically form neighborship with adjacent routers. If an attacker places a rogue router into the network which can build neighborship with the enterprise routers, he may inject rogue routes and sniff or compromise the traffic.
- **BGP** requires static neighborship definitions and is therefore more secure.

Authentication Methods

- **Plain Text Authentication**
Password is sent in clear text from one router to another.
Can be used with RIPv2, OSPFv2 or IS-IS.
- **Hashing Authentication**
Cisco recommended.
MD5 or SSH
Send **Hash Digest's**.
MD5 is supported by RIPv2, EIGRP, OSPFv2, OSPFv3, IS-IS and BGP.
SSH is supported by RIPng, Named EIGRP, OSPFv2, OSPFv3 and IS-IS.

Key Chains

- Having two routers each configured with an identical **key** (called **shared secret key**) is a basic requirement for routing protocol authentication.
- Cisco recommends to frequently change the keys.

- You can define **time-based key chains**. They contain **keys**, **key ID's**, **key lifetimes**.
- Key Chains are associated to **interfaces**.

Configuring Key Chains

```
key chain [R1KEYCHAIN]
key 1
key-string PRIMARY_KEY
accept-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
send-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
key 2
key-string SECONDARY_KEY
accept-lifetime 01:00:00 May 1 2014 infinite
send-lifetime 01:00:00 May 1 2014 infinite
```

Troubleshooting Key Chains

- ❑ **Key Number** and **Key String** must match.

```
#show key chain

#show ip eigrp neighbors
#show ipv6 eigrp neighbors          → Shows: Hold and uptime

#show ip ospf interface            → Shows:
                                   All interfaces enabled in the OSPF process
                                   Network type
                                   Hello-Timer

#show ip ospf interface [IF]      → Shows:
                                   OSPF authentication Type

show ip ospf neighbor              → Lists know neighbors and neighbor state

show crypto ipsec sa interfaces [IF]

#show ip bgp summary
#show bgp ipv6 unicast summary     → Shows:
                                   BGP router ID,
                                   Configured BGP neighbors and their ASN
```

EIGRP Authentication

- EIGRP authentication causes routers to authenticate every EIGRP message using **preshared key (PKS)**.
- If the authentication fails, the routers can't become neighbors because they will drop the EIGRP Hello messages.
- EIGRP authentication helps prevent **denial of service (DoS)** attacks.
- EIGRP supports **SHA** and **MD5** for authentication.

Configuring EIGRP Authentication (IPv4)

```
key chain [R1KEYCHAIN]
key 1
key-string PRIMARY_KEY
accept-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
send-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
key 2
key-string SECONDARY_KEY
accept-lifetime 01:00:00 May 1 2014 infinite
send-lifetime 01:00:00 May 1 2014 infinite

ip authentication mode eigrp [ASN] md5
ip authentication key-chain eigrp [ASN] [R1KEYCHAIN]
```

Configuring EIGRP Authentication (IPv6)

```
key chain [R1KEYCHAIN]
key 1
key-string PRIMARY_KEY
```

```

accept-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
send-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
key 2
key-string SECONDARY_KEY
accept-lifetime 01:00:00 May 1 2014 infinite
send-lifetime 01:00:00 May 1 2014 infinite

ipv6 authentication mode eigrp [ASN]md5
ipv6 authentication key-chain eigrp [ASN] [R1KEYCHAIN]

```

Configuring Named EIGRP Authentication

```

key chain [R1KEYCHAIN]
key 1
key-string PRIMARY_KEY
accept-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
send-lifetime 01:00:00 April 1 2014 01:00:00 May 2 2014
key 2
key-string SECONDARY_KEY
accept-lifetime 01:00:00 May 1 2014 infinite
send-lifetime 01:00:00 May 1 2014 infinite

(config-router-af-interface)#authentication mode [md5|hmac-sha-256] [0-7] [pwd]
authentication key-chain [R1KEYCHAIN]

```

OSPF Authentication

- OSPF authentication causes routers to authenticate every OSPF message using preshared key (PKS).
- OSPF authentication can be enabled on *individual interfaces* or an *entire area*.

OSPF Authentication Types

Type 0 Does not provide any authentication
Type 1 Provides plain text authentication
Type 2 Provides hashing authentication

Configuring OSPFv2 Plain Text Authentication

- The max. length of the authentication key is eight characters.

```

ip ospf authentication-key KEYLIME
area 0 authentication
-----
ip ospf authentication message-digest

```

Configuring OSPFv2 MD5 Authentication

- The max. length of the authentication key is 16 characters.

```

ip ospf message-digest-key 1 md5 KEYLIME
(config-router)#area 0 authentication message-digest

```

Configuring OSPFv3 Authentication

- OSPFv3 has *no authentication field* in its header, it relies on *IPSec* to provide authentication and encryption.
- In IPSec, there is a *Authentication Header (AH)* and an *Encapsulation Security Payload (ESP)*.
- You need to specify a *Security Policy Index (SPI)* and a Key String.

```

area 0 authentication ipsec spi 256 sha1 [x]
ipv6 ospf authentication ipsec spi 256 sha1 [x]

```

BGP Authentication

- BGP authentication is going through *MD5*.

```

neighbor [IP] password [KEYNOTE]

```

BGP IPv6 Authentication

- BGP authentication is going through **MD5**.

```
neighbor [IPv6] password [KEYNOTE]
```

Access Control Lists

- ACLs can also be used to protect the routers **management plane** and the **control plane**.
- See **time-based ACLs** and **infrastructure ACLs**.

uRPF - Unicast Reverse Path Forwarding

- One option to prevent malicious traffic from entering a network is to use **uRPF**.
- The way that **uRPF** works is to check the **source IP address** of a packet arriving on an interface and determine **whether that IP address is reachable**, based on the router's **FIB**, used by **CEF**.
- **CEF** must be enabled on a router to use **uRPF**.
- **uRPF** does not support **ACL templates**.

uRPF Modes

Strict Checks **source IP** and **arriving interface**.

Assure there is no chance of **asynchronous routing**, otherwise strict mode will drop traffic.

By **default**, a router with uRPF configured would drop a packet whose source IP address is only reachable by a **default route**.

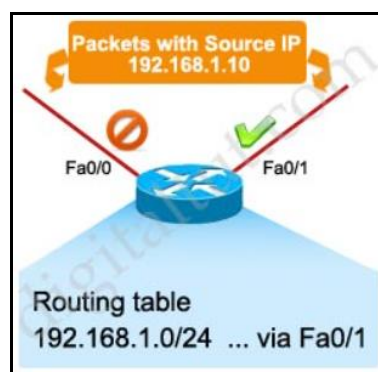


Figure 25: uRPF - Strict Mode

Loose Checks only source IP

VRF uRPFv3 mode.

Configuring uRPF

Strict Mode

```
ip verify unicast source reachable-via rx
ip verify unicast source reachable-via rx allow-default
ip verify unicast source reachable-via rx allow-self-ping
```

Loose Mode

```
ip verify unicast source reachable-via any
ip verify unicast source reachable-via any allow-default allow-self-ping
```

Troubleshooting uRPF

```
#show cef interface
```

→ Verify if uRPF is enabled

```
#show cef interface s0/0
```

AAA - Authentication, Authorization and Accounting

- With AAA services, you can have a **single repository** for user credentials.
- Users can quickly be **added** and **deleted** from the AAA database **without the need to reconfigure each router**.
- The **Self-contained AAA** method is also known as **local authentication**.
- There are **3** services of AAA.

Authentication

- The authentication service checks **user credentials** to confirm he is who he claims to be.
- Supports a **local database**.

Authorization

- After being authenticated, the authorization service determines **what that user can do**.
- Enforces **time periods** during which a user can access the device.
- Defines **EXEC mode commands**.
- Defines **network connections** such as **PPP, SLIP, ARAP**.

Accounting

- The accounting service can **collect** and **store** information about a user's login.
- This information can be used, for example, to keep an **audit trail** of what a user did on the network.
- Logging amount of **network resources** that users are consuming.
- Verifies **network usage**.
- **Reports** user's activity to the TACACS+ or RADIUS server.
- Accounting information's can be sent to a maximum of **4 AAA servers**.
- Uses **Named Method** lists.
- System accounting does not use **named accounting lists**.
- Not supported with local AAA.

Accounting Types:

- Network Accounting
- EXEC Accounting
- Command Accounting
- Connection Accounting
- System Accounting
- Ressource Accounting
- VRRS Accounting

Characteristic	TACACS+	RADIUS
Transport layer protocol	TCP	UDP
Modularity	Provides separate services for authentication, authorization, and accounting	Combines authentication and authorization functions
Encryption	Encrypts entire packet	Only encrypts the password
Accounting functionality	Offers basic accounting features	Offers robust accounting features
Standards-based	No (Cisco-proprietary)	Yes

Figure 26: TACACS+ and RADIUS Server

Configuring AAA

```
aaa new-model
aaa authentication login ADMIN group tacacs+ local
username [name] secret [pwd]
tacacs server [X]
address ipv4 [IP]
key [x]
line vty 0 4
login authentication [ADMIN]
=====
aaa authorization exec default local
```

Troubleshooting AAA

#show running-config aaa

SNMP Security

Versions: SNMPv1, SNMPv2, SNMPv2c, SNMPv3

- The security integrated with **SNMPv1** and **SNMPv2** is considered weak.
- The **community-string** is like a password.
- Change the **community-strings** to nondefault values!
snmp-server community [x] ro 10
- Add an **ACL** with trusted management stations.

Component	Description
SNMP manager	An SNMP manager runs a network management application. This SNMP manager is sometimes referred to as a Network Management Server (NMS).
SNMP agent	An SNMP agent is a piece of software that runs on a managed device (for example, a server, router, or switch).
Management Information Base (MIB)	Information about a managed device's resources and activity is defined by a series of objects. The structure of these management objects is defined by a managed device's Management Information Base (MIB).

Figure 27: SNMP Components

Security Model	Security Level	Authentication Strategy	Encryption Type
SNMPv1	noAuthNoPriv	Community string	None
SNMPv2c	noAuthNoPriv	Community string	None
SNMPv3	noAuthNoPriv	Username	None
SNMPv3	authNoPriv	MD5 or SHA-1	None
SNMPv3	authPriv	MD5 or SHA-1	DES, 3DES, or AES

Figure 28: SNMP Security Models

Options:

NoAuthNoPriv

→ No security is configured

MANAGING A CISCO INTERNETWORK

ROM	Bootstrap, POST routine, Mini IOS, ROM monitor
RAM	running-config , ARP cache, Routing tables, Packet buffers
NVRAM	startup-config , is not erase when the router is reloaded
Flash Memory	IOS Software , is not erased when the router is reloaded

INTERNAL COMPONENTS OF A CISCO ROUTER AND SWITCH

The default order of an IOS loading from a Cisco device begins with **Flash**, the **TFTP server**, and finally **ROM**.

Verify IOS integrity

`show version` → Shows the flash file
`verify /md5 flash:<file>`

`#show flash`

#	length	date/time	path
1	1336	Apr 08 2010 01:17:54	nvrाम
2	3273	Dec 01 2011 20:34:32	SDM_Backup
3	2850	Sep 12 2011 23:45:48	CCP_backup
4	1038	Apr 02 2010 04:06:16	home.shtml
5	115712	Apr 02 2010 04:06:16	home.tar
6	1697952	Apr 02 2010 04:06:16	securedesktop-ios-3.1.1.45-k9.pkg
7	415956	Apr 02 2010 04:06:18	sslclient-win-1.1.4.176.pkg
8	931840	Mar 24 2010 09:13:42	ES.TAR
9	10	Mar 24 2010 10:35:18	HOST.CFG
10	258048	Mar 24 2010 09:13:40	SDMLauncher.exe
11	2900	Apr 02 2010 04:06:14	cpconfig-2811.cfg
12	2941440	Apr 02 2010 04:06:14	cpexpress.tar
13	6646	Apr 02 2010 04:06:14	Help.htm
14	61822472	Jan 21 2011 17:49:56	c2800nm-adventerprisek9-mz.150-1.M4.bin

61521920 bytes available (68231168 bytes used)

Figure 29: #show flash

Backup a Cisco device

`copy running-config tftp`
`copy startup-config tftp`
`write-memory` → Issue in archive config mode

Restore a Cisco device

`copy tftp running-config` → Copies a file to running-config, but does not replace it.
`config replace` → Copies a file from the archive into running-config and replaces it.

Erase a Cisco device

`erase startup-config` → Deletes the content of the NVRAM

The Purpose of the Configuration Register

- The **last hexadecimal character** is used to control how the router boots.

The configuration register can be used to change router behavior in several ways, such as:

- How the router boots (into ROMmon, NetBoot)
- Options while booting (ignore configuration, disable boot messages)
- Console speed (baud rate for a terminal emulation session)

`confreg 0x2..` → Set the Configuration Register
`config-register 0x2..` → Set the Configuration Register

0x2100	Router will boot into ROMmon mode
0x2101	Boots into bootstrap , Ignores break, The first image located in flash will be booted
0x2102	The first image located in flash will be booted (Default Setting), ignores break
0x2120	Boots into ROMmon

0x2142 For Password Recovery. Ignore the startup-config file at reload (NVRAM)

show version

→ Shows configuration Register Value

Bit Number	Hexadecimal	Meaning
00-03	0x0000-0x000F	Boot field.
06	0x0040	Ignore NVRAM contents.
07	0x0080	OEM bit enabled.
08	0x0100	Break disabled.
09	0x0200	Causes system to use secondary bootstrap (typically not used).
10	0x0400	IP broadcast with all 0s.
5, 11, 12	0x0020, 0x0800, 0x1000	Console line speed.
13	0x2000	Boots default ROM software if network boot fails.
14	0x4000	IP broadcasts do not have net numbers.
15	0x8000	Enables diagnostic messages and ignores NVRAM contents.

15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0	Bit places
0	0	1	0	0	0	0	1	0	1	0	0	0	0	1	0	Register bits
2				1				4				2				Bits represented in hex
In this example, bits 13, 8, 6, and 1 are turned on. Converting these groups of four binary nibbles gives you the hexadecimal number of 0x2142.																
A nibble is half of a byte, or 4 bits.																

Dynamic Host Configuration Protocol (DHCP)

- If you get a default static route on your router from your ISP, this route is called a **"floating static route"** and has an administrative distance (AD) of **254**.

DHCP Options

See: <http://networksorcery.com/enp/protocol/bootp/options.htm>

- 43** Vendor specific information.
e.g. Cisco Wireless Lan Controller used to return the address of the **master controller**.
- 66** TFTP server name (e.g. for VoIP-Phones)
- 82** Relay Agent Information
- 128** TFTP Server IP address
- 150** TFTP server address

Configuring DHCP

- Exclude the reserved/excluded addresses
ip dhcp excluded-address 192.168.10.1 192.168.10.10
- Create a pool for each LAN
ip dhcp pool [Sales_Wireless]
- Choose the network ID and subnet mask for the DHCP pool that the server will use to provide addresses to hosts
network 192.168.10.0 255.255.255.0
- Add the default gateway
default-router 192.168.10.1
- Provide the DNS servers
dns-server 4.4.4.4
- Provide the Domain name
domain-name [x]
- Set the lease time
lease 0 1 → 1h
lease 3 12 15 → 3d 12h 15m

- Store DHCP bindings for addresses already leased and not stored on DHCP-Server
`ip dhcp database`

`(config)#no ip dhcp client request router` → Prevents the assignment of a static route.

Configuring DHCP-Relay

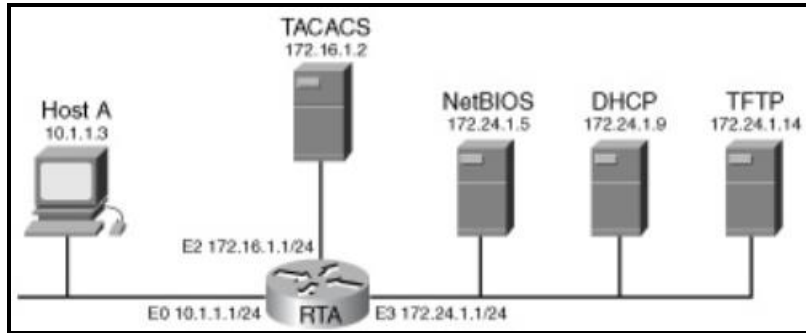


Figure 30: IP Helper Address

```
RTA(config)#interface e0
RTA(config)#ip helper-address 172.24.1.9
```

 Configure the Stateful IPv6 DHCP Relay Agent
`(config-if)#ipv6 dhcp relay destination [IP] [IF]`

`service dhcp` → Enables the DHCP relay agent feature

Troubleshooting DHCP

- `#show ip dhcp binding`
To detect IP conflict.
Shows IP addresses already assigned.
- `#show ip dhcp pool [poolname]`
Total numbers of addresses leased
- `#show ip dhcp server statistics`
- `#show ip dhcp conflict`
- `#show ip dhcp database`
Database agent informations such as: Location, Status of connectivity
- `#show ip interface`
Shows the DHCP-Relay agent
- Use the debugging function on the IOS
`#debug ip dhcp server packet`

Network Time Protocol (NTP)

RFC 5904

Transport: By default, NTP communications use **UDP port 123**.

Link: [Public NTP-Servers](#)

- NTP version 4 (NTPv4)** is the latest and preferred version of NTP.
- Cisco routers** currently only support through version 3 (14.11.2016).
- Four different modes: **client**, **server**, **peer** and **broadcast**.

- The **Stratum level** defines the quality of the clock source. The **lower** the stratum, the better the source. **Lower stratum levels** are considered more authoritative.
- **Stratum 1 server**, directly connected to radio receivers or atomic clocks.
- **Stratum 2 server**, is one that gets its time information from a stratum 1 server.
- **Recommendation**: Use three internal NTP-Servers, synchronized with 3 different external NTP-Servers.
- Stratum Level **1-15**
- Stratum Level **16** indicates that the device does not have its time synchronized.
- Default ??? (8 or 16)
- NTPv4 provides **IPv6 support** and better **security**.

Configuring NTP

1. Setup NTP on **clients**
(config)#ntp server 172.16.10.1 [version 4]

```
-----  
(config-if)#set ntp broadcastclient enable
```

2. To set the router or switch as **NTP-Server**
ntp master [x]

3. Setup a Syslog server
logging host 172.16.10.1

4. service timestamps log datetime msec

SERVE

- Allows time requests and NTP control queries, but does not allow the system to synchronize to the remote system.

```
ntp access-group serve [ACL]
```

PEER

- Allows time requests and NTP control queries and allows the system to synchronize to the remote system.

```
ntp access-group peer [ACL]
```

Troubleshooting NTP

```
#show ntp status  
show ntp associations  
show ntp associations detail
```

NTP Authentication

Configuring NTP Server Authentication

```
ntp authentication-key [x] md5 [key]  
ntp authenticate  
ntp trusted-key [key-id]  
(config-line)#ntp master [stratum]
```

→ Enables the NTP authentication feature

Configuring NTP Client Authentication

```
ntp authentication-key [x] md5 [key]  
ntp authenticate  
ntp trusted-key [key-id]  
ntp server [IP] key [key-id]
```

CDP - Cisco Discovery Protocol

- Works on LLC-Level (OSI-Layer 2).
- Can display **Layer 3** information's even though working on **Layer 2**

- **CDP is enabled** on Cisco devices by **default**

Configure CDP

- Enable CDP first globally

Troubleshooting CDP

```
#show cdp
[no] cdp run                → Affects CDP globally
[no] cdp enable            → Affects only the interface
cdp holdtime
cdp timer
#show cdp traffic
#show cdp neighbors        → One line per neighbor
#show cdp neighbors detail → Shows also Layer 3 information's (IP)
```

```
SW2# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID         Local Intrfce   Holdtme    Capability   Platform   Port ID
SW1                Gig 0/2         170        S I          WS-C2960-  Gig 0/1
R1                 Fas 0/13        136        R S I        CISCO2901 Gig 0/1
```

Figure 31: show cdp neighbors

```
SW2# show cdp neighbors detail
-----
Device ID: SW1
Entry address(es):
  IP address: 172.16.1.1
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/2, Port ID (outgoing port): GigabitEthernet0/1
Holdtime : 161 sec

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version 15.0(1)SE3, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2012 by Cisco Systems, Inc.
Compiled Wed 30-May-12 14:26 by prod_re1_team

advertisement version: 2
Protocol Hello: OUI=0x00000C, Protocol ID=0x0112; payload len=27,
  value=00000000FFFFFFFF010221FF000000000000018339D7B0E80FF0000
VTP Management Domain: ''
Native VLAN: 1
Duplex: full
Management address(es):
  IP address: 172.16.1.1
```

Figure 32: show cdp neighbors detail

Link Layer Discovery Protocol (LLDP)

Protocol: 802.1AB

- Works like CDP
- Based on IEEE 802.1ab standard
- LLDP works in multivendor networks
- By default LLDP is globally disabled on a Catalyst switch

```
#show lldp
#show lldp neighbors
#show lldp neighbors [IF] detail
(config)#lldp run
(config)#lldp receive
```

Telnet

```
telnet x.x.x.x
```

Troubleshooting BGP

```
telnet x.x.x.x 179 /source-interface loopback 0
```

Troubleshooting HTTP

```
telnet x.x.x.x 80  
GET /default.htm HTTP/1.1
```

Troubleshooting IMAP4

```
telnet x.x.x.x 143  
a001 login username pwd  
a002 select inbox  
a003 fetch 274 body[header]  
...  
a002 fetch 1:279 ALL → List all headers from 1 to 279  
...  
a004 store 274+flags \deleted → Delete the Email  
a005 logout
```

Troubleshooting IPv6

```
telnet 2000:a::1  
telnet 2000:a::1 80
```

Troubleshooting POP3

```
telnet x.x.x.x 110  
USER <account name>  
PASS <pwd>  
LIST or LIST #  
RETR <msg-no>  
QUIT
```

Troubleshooting SMTP

```
telnet x.x.x.x 25  
helo mailhost.domain.tld  
mail from:sender@domain.com  
rcpt to:receiver@domain.com  
data  
Subject: Test SMTP  
... blank space row  
...Text  
end with a dot!  
quit
```

IP ROUTING

Routing occurs when a router or some Layer 3 device makes a forwarding decision based on network address information.

The frame changes at each hop but the packet never changes.

A MAC address will only be used on local LAN. It will never pass a router's interface.

- Process Switching
- Fast Switching
- Cisco Express Forwarding (CEF)

Router Configuration

- hostname
hostname <X>
- passwords
- interface
- descriptions
description [your router description]
- banners

Static Routing

- Manually configured at the CLI.
- For smaller network topologies, OK.

PROS

- No CPU overhead
- No bandwidth usage
Needs very little space 16 octets with just 3 kb of overhead.
- Additional security

CONS

- You can make errors
- Administrative work

```
ip route [dest-netID] [mask] [next-hop_rtr | exitIF] [adm-dist] [permanent]
```

```
ip route 192.168.10.0 255.255.255.0 [NH] → NetID + mask plus next hop [NH]
```

```
ip route 192.168.10.0 255.255.255.0 [NH] [AD] → NetID + mask plus next hop [NH] + Adm. Dist. [AD]
```

```
ip route 0.0.0.0 0.0.0.0 [NH] → Default Gateway / Gateway of last resort
```

The **set ip default next-hop** command

- Verifies the existence of the destination IP address in the routing table, and...
 - if the destination IP address exists, the command does **not policy route** the packet, but forwards the packet based on the **routing table**.
 - if the destination IP address does not exist, the command **policy routes** the packet by sending it to the specified next hop.

```
(config-route-map)#set ip default next-hop
```

The **set ip next-hop** command

- Uses a Route-Map
- Verifies the existence of the next hop specified, and...
 - if the next hop exists in the routing table, then the command **policy routes** the packet to the next hop.
 - if the next hop does not exist in the routing table, the command uses the **normal routing table** to forward the packet.

```
(config-route-map)#set ip next-hop
```

Default Routing

- Where a special route is configured for all traffic without a more specific destination network found in the routing table.

Gateway of last resort

```
ip route 0.0.0.0 0.0.0.0 [ip-address]
```

OSPF

```
default-information originate → Creates a Type-5 LSA
```

Dynamic Routing

Routers are sharing routing information's via a routing protocol.

- Routing Information Protocol (**RIP**) Ver. 1 & 2
Distance Vector protocol
Makes decisions based on hop count.

```
Cmd:  config t
      (config)#router rip
      (config-router)#network 10.0.0.0
      (config-router)#network 172.16.0.0
      version 2
      no auto-summary
```

- **Interior Gateway Protocol (IGP)**
 - IGPs are used to exchange routing information with routers in the **same autonomous system (AS)**.
 - Automatic discovery of peers.
 - Generally, trust your IGP routers.
 - Routes go to all IGP routers.
 - Modern IGP protocols use **multicast**.
- **Exterior Gateway Protocol (EGP)**
 - EGPs are used to communicate **between ASs** (e.g. BGP).
 - Specifically, configured peers.
 - Connecting with outside networks.
 - Set administrative boundaries.

Routing Protocols

Route update packets are used to help **build and maintain routing tables**.

Classless Routing-Protocols (using CIDR):

OSPF, EIGRP, RIPv2, IS-IS, BGP

Classful Routing-Protocols

RIPv1, IGRP

Distance Vector

RIPv1, RIPv2, RIPv2, IGRP, Babel, EIGRP, DSDV

- A distance vector protocol sends a **full copy** of its routing table to its directly attached neighbors.
- To prevent routing loops usually **Split Horizon** or **Poison Reverse** are used.

Link State

OSPF, IS-IS

- A link-state routing protocol allows routers to build a **topological map** of a network.
- The algorithm is Dijkstra's Shortest Path First.
- Only topology updates are advertised after the adjacency is build.

Path Vector Protocol

BGP, BGP-4, MP-BGP

- Includes information about the exact path packets take to reach a specific destination network.

Characteristic	OSPF	RIPv2	RIPv1
Type of protocol	Link state	Distance vector	Distance vector
Classless support	Yes	Yes	No
VLSM support	Yes	Yes	No
Auto-summarization	No	Yes	Yes
Manual summarization	Yes	Yes	No
Noncontiguous support	Yes	Yes	No
Route propagation	Multicast on change	Periodic multicast	Periodic broadcast
Path metric	Bandwidth	Hops	Hops
Hop count limit	None	15	15
Convergence	Fast	Slow	Slow
Peer authentication	Yes	Yes	No
Hierarchical network requirement	Yes (using areas)	No (flat only)	No (flat only)
Updates	Event triggered	Periodic	Periodic
Route computation	Dijkstra	Bellman-Ford	Bellman-Ford

Hybrid- / Advanced Distance Vector

EIGRP

Administrative Distance (AD)

- The AD is a local setting on a router and cannot be advertised to neighboring routers.

0	Connected Interface
1	Static Route
5	Enhanced Interior Gateway Routing Protocol (EIGRP) summary routes
20	eBGP (external router)
90	EIGRP (internal router)
100	IGRP
110	OSPF
115	IS-IS
120	RIP
140	Exterior Gateway Protocol (EGP)
160	On Demand Routing (ODR)
170	EIGRP (external routers)
200	iBGP (internal router)
254	Floating static route (usually if DHCP for ISP is used)
255	Not usable (this route will never be used)

AD setting with the distance command:

```
RIP (config-router)#distance [ad-value]
EIGRP (config-router)#distance eigrp [internal-ad] [external-ad]
OSPF (config-router)#distance ospf [external-ad intra-area-ad-value
inter-area-ad-value]
```

RIPv1

Routing-Protocol.

- RIPv1 is a **classful** routing protocol
- RIPv1 was the first routing protocol.
- RIP is using the number of **Hops** to calculate the best route.
- Maximum allowable hop counts **15**
- RIPv1 doesn't send updates with subnet
- RIP-Updates every **30 sec.** (Default)
- Hold time **180 sec.** (Default)
- Invalid after **180 sec.** (Default)
- Flushed after **180 sec.** (Default)
- Default seed metric **INFINITY** = 0.
- Uses **broadcast**.

Configure RIPv1

```
router(config)#router rip
router(config)#version 1
router(config)#network address
```

RIPv2

Transport: Uses UDP port **520**

- Provides **prefix routing**.
 - RIPv2 sends subnet mask information's (**CIDR**).
- RIPv2 is a **classless routing protocol**
- Uses **split horizon** as a loop prevention mechanism
- It supports **MD5** and **plaintext authentication**
- Default seed metric **INFINITY** = 0.
- Maximum allowable hop counts **15**
- Uses **multicast**.

Configure RIPv2

```
(config)#router rip
(config-router)#version 2
(config-router)#network [address] → No subnetmask!

no auto-summary
maximum-paths [4] → Maximum equal routes for a single destination (default 4)
passive-interface default → Sends no updates out on all interfaces
no passive-interface s0/0/0 → Enables the interface to send updates
```

RIPng

RFC 2080

Transport: RIPng sends updates on **UDP port 521** using the multicast group **FF02::9**.

RIPng (RIP next generation), defined in RFC 2080, is an extension of RIPv2 for support of IPv6, the next generation @Internet Protocol.

The main differences between RIPv2 and RIPng are:

- Distance vector protocol with a max hop count of **15**
- Support of **IPv6 networking**.
- While RIPv2 supports RIPv1 updates authentication, RIPng does not. IPv6 routers were, at the time, supposed to use IPsec for authentication.
- RIPng uses **IPv6 AH/ESP** for authentication, relying on IPsec.
- RIPv2 encodes the next-hop into each route entry, RIPng requires specific encoding of the next hop for a set of route entries.
- Does not support **automatic summarization**
- It **converges** relatively slow in comparison to EIGRP and OSPF.

- RIPng allows **multiple RIPng processes** on a single router
- It doesn't advertise routes for **IPv4**.
- Default seed metric **INFINITY** = 0.
- RIPng can only be enabled under the **interface configuration mode**.
- To communicate between neighbors, the **link-local unicast IPv6** address is used.

RIPng Default Timers:

Update: 30 seconds

Expire: 180 seconds

Flush: 240 seconds

Configuring RIPng

```
(config)#ipv6 unicast-routing
(config)#ipv6 router rip [name]
(config-if)#ipv6 address [address/prefix] [eui-64]
(config-if)#ipv6 rip [name] enable
```

Inject the IPv6 default route ::0

```
(config-if)#ipv6 rip [PID] default-information originate
```

```
ipv6 rip [process-name]
```

Troubleshooting RIPng

- The RIPng routing process will be automatically created when you enable RIPng on the first interface.
- The process name does not have to match.

```
#show ipv6 rip → Show all RIPng routing processes
#show ipv6 rip database
#show ipv6 interface brief → Status and addressing assignments

#show ipv6 route
#show ipv6 route rip
show ipv6 route [prefix/length]
#show ipv6 protocols → Lists the interfaces on which RIPng is enabled.
#show ipv6 rip next-hops

#clear ipv6 rip

debug ipv6 rip

show cdp entry [name]
```

IS-IS

Intermediate System to Intermediate System.

- **Link-state protocol**, needs a hierarchical IP addressing scheme for optimal functionality
- There is a high demand o **router resources** to run a link-state protocol.

Troubleshooting ROUTES

- Interface must be up/up
show ip int brief
- [1/0]** means
1 = Administrative distance
0 = Metric

```
show ip route
show ip route [ip]
show ip route connected
show ip potocols
```

EVN - Cisco Easy Virtual Network

- ***EVN*** is the newer approach of ***VRF-Lite***.
- Dramatically ***simplifies*** the relatively complex ***configuration*** required by ***VRF-Lite***.
- Uses a ***Virtual Network Trunk (VNET Trunk)*** to carry traffic for each virtual network, and eliminates the need to manually configure a subinterface for each virtual network on all routers.
- VNET trunk is using ***VNET tags (802.1Q)*** to identify the packets.
- EVN supports ***OSPFv2*** and ***EIGRP***.
- Shares ***IP address, routing table*** and ***forwarding table*** on the subinterfaces.
- Separation for networks over a common infrastructure.
- Subnets are crossing routers.
- ***Traffic separation*** and improved ***network efficiency***.
- The ***route replication service*** allows IP routes known to one virtual network to be known to other virtual networks. For example if one VRF contains services like DNS or DHCP, router replication can be used to add this VRF route into other VRF's.

LAYER 2 SWITCHING

Layer 2 switching is the process of using the hardware address of devices on a LAN to segment a network.

- The biggest benefit gained by having a layer 2 switched network is that it creates individual *collision domain* segments.
- Notice there are *access ports* for each host and *access port* between switches - one for each VLAN.
- Switches *remove* any VLAN information from the frame before it's forwarded out to an *access-link device*. Or they drop packets with 802.1Q tags.
- Nowadays, most switches will allow you to add a *second VLAN to an access port* for your *voice traffic*, called the *voice VLAN / Auxiliary VLAN*. This allows you to connect both a phone and a PC device to one switch port but still have each device in a separate VLAN.
- *Trunk ports* can carry multiple VLANs at a time. *1-4094* VLANs. But the amount is only up to *1001* unless you're going with something called *extended VLANs*. This is a great feature because you can set ports up to have a server in two separate broadcast domains simultaneously so your users won't have to cross a layer 3 device (router) to log in and access it. *Trunk ports* support tagged and untagged traffic simultaneously.
- *Switch fabric*, a group of switches that share the same VLAN information.
- Performs *transparent bridging* Layer 2 switch.

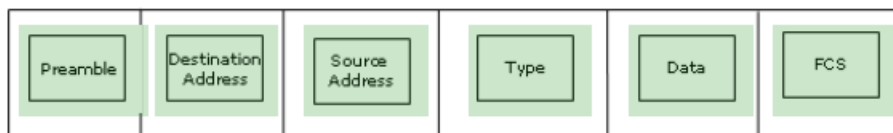


Figure 33: Ethernet Frame

Address learning

- When a switch is first powered on, the MAC forward/filter table (CAM) is empty.
- When receiving frames, the switch updates the MAC table with the source address (MAC)
- If hosts don't communicate to the switch again within a certain time period, the switch will flush their entries from the database to keep it as current as possible.

Forward/filter decision

```
#show mac address-table
```

EtherChannel

EtherChannel is a *port link aggregation technology* or port-channel architecture used primarily on Cisco switches. It allows grouping of several physical Ethernet links to create one logical Ethernet link for providing fault-tolerance and high-speed links between switches, routers and servers.

Source: Wikipedia

- Note, that once you setup EtherChannel, STP a layer 3 routing protocols will treat those bundled links as a *single one*.
- Cisco's EtherChannel can bundle up to *eight ports* to provide resiliency and more bandwidth between switches.

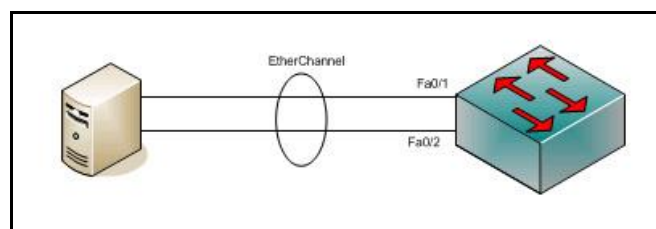


Figure 34: EtherChannel

- Cisco: Port-Aggregation-Protocol (*PAgP*)
Sends packets *every 30 seconds* to manage the link

- IEEE: Link-Aggregation-Control-Protocol (**LACP, 802.3ad**)
Active and Standby links.
More optional features than PAgP.
- Ethernet frames shouldn't be mixed up in **sequence**.
- EtherChannel load balances by **flows**.
- Best praxis is to use Dynamic Negotiation such as **PAgP** or **LACP**.

Configuring EtherChannel

```
(config)#int range g0/1-2
(config-if-range)#switchport trunk encapsulation dot1q
(config-if-range)#switchport mode
(config-if-range)#switchport trunk allowed vlan 1,2,3
```

```
(config-if-range)#channel-group 1 mode active
(config-if-range)#channel-group 1 mode desirable
```

```
(config-if-range)#switchport mode trunk
(config-if-range)#channel-protocol lacp
(config-if-range)#channel-group 1 mode passive
```

Troubleshooting EtherChannel

- Same Port speed, Duplex and VLAN information must be used between the switches.

```
#show running-config
#show interface trunk
```

```
#show etherchannel summary           → Displays one line of information per port
#show etherchannel x summary
#show etherchannel port-channel
#show etherchannel load-balance
```

PortFast

- By **default**, PortFast is **disabled** on all switch ports.
- With PortFast a switch may change from Blocking-Mode to Forward-Mode **without Listening- and Learning-Mode**.
- Enables **fast connectivity** to be established on access layer switch ports to **workstations** that are booting.
- Port Fast reduces the usual port initialization **50 seconds** converge time of **STP**.
- 30 seconds are due to **STP transitions**.
- PortFast is used only for user-devices on **Access-Ports**. If a user starts his device, the port may switch directly into Forwarding-Mode.
- If you turn on PortFast for a switch port, it's a good idea to turn on **BPDU Guard** as well.
- By definition, if you enable PortFast, you do **not expect** to find anything that can cause a **bridging loop**.

```
(config-if)#spanning-tree portfast
(config-if)#no spanning-tree portfast
```

UplinkFast

- Enables fast-uplink failover on an **access layer switch** when dual uplinks are connected into the distribution layer.

```
#show spanning-tree uplinkfast
```

```
(config)#spanning-tree uplinkfast [X]
```

BackboneFast

- Enables **fast convergence** in the network backbone or core layer switches after a spanning-tree topolog change occurs.
- Can reduce the maximum convergence delay only **from 50 to 30 seconds**.
- When used, BackboneFast should be enabled on **ALL switches in the network**.

```
#show spanning-tree backbonefast
(config)#spanning-tree backbonefast
```

BPDU Guard - Bridge Protocol Data Unit Guard

- Deactivates BPDU on certain ports and avoids with this, that a hacker can become **Root-Switch** with his device.
- There is a **12-bit field** (sys-id-ext) inserted into an Ethernet frame to define VLANs in an STP instance.
- there are two types of BPDU:
 - Configuration BPDU
 - Topology Change Notification (TCN) BPDU
- By **default**, BPDUs are sent out all switch ports every **2 seconds**.
- By **default**, BPDU Guard is **disabled** on all switch ports.
- You should use BPDU Guard on all switch ports where STP **PortFast** is enabled.
- The BPDU Guard feature was developed to further protect the integrity of switch ports that have **PortFast enabled**.
- An obvious application for BPDU Guard is on **access layer switch ports** where users and end devices connect.
- You never should enable BPDU Guard on any **switch uplink** where the root bridge is located.

```
(config)#spanning-tree portfast bpduguard default
(config-if)#spanning-tree portfast bpduguard enable
```

BPDU Filtering

- By **default**, BPDU Filtering is disabled on all switch ports.
- If **PortFast** is disabled on a port, then BPDU filtering will not be enabled there.
- Enable BPDU filtering only if the connected device cannot allow BPDUs to be accepted or sent.
- BPDU filtering stops all BPDUs from being received or sent on a switch port, effectively **disabling STP**.

```
(config)#spanning-tree portfast bpdupfilter default
```

Root Guard

- Can only be enabled on a **per-port basis**.
- By **default**, it is **disabled**.
- Use Root Guard on switch ports where **you never expect** to find the root bridge for a VLAN.

```
#show spanning-tree inconsistentports
```

```
(config-if)#spanning-tree guard root
```

Port Security

- Shut down unused ports or assign an unused VLAN to them.
- Set the port to access otherwise no port-security setting is possible

Secure MAC addresses:

- **Static secure MAC address**
These MAC addresses are manually added to the MAC address table using the **switchport port-security mac-address mac-address** command. You can use the

`no switchport port-security mac-address` command to remove any static secured MAC address.

- **Dynamic secure MAC address**

These MAC addresses are dynamically added to the MAC address table. They are automatically removed from the MAC address table when the switch is restarted. You can use the `clear port-security dynamic address` command to remove any one dynamic secure MAC address and the `clear port-security dynamic interface` command to remove all dynamic secure MAC addresses on an interface.

- **Sticky secure MAC address**

These MAC addresses are added to the switch's MAC address table and to the switch's running-configuration. If the configuration is stored, these MAC addresses will remain in the switch configuration even when the switch restarts. You can use the `no switchport port-security mac-address sticky` command to disable the sticky learning of MAC addresses by the switch.

3 Port Security Modes:

- **Protect**

In this mode the packets with unknown source addresses are dropped when the secure port has reached its configured maximum number of secure MAC addresses. These packets are dropped until the number of secure MAC addresses drops below the max. configured value.

- **Restrict**

This mode causes the security violation counter to increment and sends a SNMP trap when an address-security violation occurs.

- **Shutdown (Default)**

This is the default mode. In this mode, the secure port enters an **error-disabled state**. You can re-enable the port by entering the `shutdown` and `no shutdown` interface configuration commands on the disabled interface.

Option on the switchport port-security violation Command	Protect	Restrict	Shutdown*
Discards offending traffic	Yes	Yes	Yes
Sends log and SNMP messages	No	Yes	Yes
Increments the violation counter for each violating incoming frame	No	Yes	Yes
Disables the interface by putting it in an err-disabled state, discarding all traffic	No	No	Yes

Figure 35: Port Security Modes

Configure Port-Security

```
(config)#int f0/1
(config-if)#switchport mode [access | trunk]
(config-if)#switchport port-security [shutdown | restrict | Protect]
```

`switchport port-security maximum 1` → Allows only one MAC address on that port
`switchport port-security violation shutdown`

```
switchport port-security mac-address sticky
switchport port-security maximum 2
switchport port-security violation shutdown
```

Protecting one MAC

```
switchport port-security
switchport port-security violation restrict
switchport port-security maximum 1 → Done by default using <port-security>
switchport port-security mac-address aa.bb.cc.dd.ee.ff
```

Protecting ports f0/3 and f0/4

```
(config)#int range f0/3-4
```

```
switchport mode access
switchport port-security
Check: show port-security int f0/3
```

```
-----
switchport port-security violation shutdown
switchport port-security violation protect
```

Troubleshooting Port-Security

```
show mac address-table count      → Lists MAC addresses associated with ports that use port-
show mac address-table secure     → Lists MAC addresses associated with ports that use port-
                                   security
show mac address-table static     → Lists MAC addresses associated with ports that use port-
                                   security, as well as any other statically defined MAC
                                   addresses
show port-security               →
show port-security interface [IF] →
```

LAN-Switching

The 3 components of the LAN-Switching are:

- Devices with Ethernet-Network cards (NIC's)
- Ethernet LAN Switches
- Cables

Trunk Types (802.1Q)

- access
- dynamic auto
- trunk (Router-on-a-Stick "ROAS")
- dynamic desirable mode

Decisions to be taken by a switch

- **Forward/Filter** the frame
- **Flood** the frame
- **Drop** the frame

Step 1

Access-Port: Get Access-VLAN of the interface.

Trunk-Port: Get VLAN from Trunking-Header

Step 2

The Switch adds the sender MAC-Address to the MAC-Address table and connects it with the VLAN-ID.

Step 3

The Switch searches for the receiver MAC-Address in the MAC-Address table with the VLAN-ID detected in step 1.

Match: Frame will be forwarded over the specific interface.

No Match: Frame will be flooded over all Access-Ports which are supporting this VLAN.

Store-and-Forward

- Switching technology
- Good frames are regenerated when they are forwarded or transmitted

Transparent Bridging

- A bridge segments only **collision domains**, it does not segment **broadcast domains**.
- **Unknown unicast** means the bridge does not find the destination MAC address in its CAM table and handles the frame as it would be a broadcast and floods it out all remaining ports.

Multilayer Switching

Route caching

- Also known as NetFlow LAN switching
- Flow-based or demand-based switching

Topology based

- This type of MLS is known as CEF.

Configuration Catalyst Switch

- Console ports are typically located on the back of the switch
- Use crossover cables to connect switches
- There are no AUX ports on Cisco switches!
- Configure an IP address for the switch for *in-band management* (Telnet, SSH, SNMP)
- Shut down unused ports or assign them to an unused VLAN
- Set the default gateway

Config the Switch S1

```
(config)#hostname [s1]
enable secret [sw1]
int f0/15
description 1st connection to [sw2]
...
description connection to IVR
line con 0
password console
login
line vty 0 15
password telnet
login
int vlan 1
ip address x.x.x.x m.m.m.m
no shut
exit
banner motd #Switch S1
exit
copy run start
```

→ On layer 2 switch address can only be set on VLAN 1

```
(config)#ip default-gateway x.x.x.x → Sets the default Gateway
```

Configuring SSH

```
ip domain-name [name]
username [name] password [pwd]
```

Troubleshooting Catalyst Switch Configuration

```
#show running-config → Time consuming to check!
#show int vlan 1 →
#show mac address-table →
```

```
mac address-table static aaaa.bbbb.ccc vlan 1 int fa0/7
```

Interface Statuses

```
show interfaces status [err-disabled]
#show ip interface brief
```

```
R3>show ip interface brief
Interface IP-Address OK? METHOD Status Protocol
FastEthernet0/0 10.3.0.1 YES NVRAM up up
FastEthernet0/1 unassigned YES NVRAM administratively down down
Serial10/0/0 10.51.0.2 YES NVRAM up up
Serial10/0/1 10.52.0.2 YES NVRAM up up
```

Line Status (Layer 1)

```
administratively down
down
```

→ Taken down by administrator (shutdown)

→ Physical connection problem/No cable installed?

up
 monitor
 err-disabled

Protocol Status (Layer 2)

up
 administratively down →
 down →
 monitor
 err-disabled

Line Status	Protocol Status	Typical Reasons
Administratively down	Down	The interface has a shutdown command configured on it.
Down	Down	The interface is not shutdown, but the physical layer has a problem. For example, no cable has been attached to the interface, or with Ethernet, the switch interface on the other end of the cable is shut down or the switch is powered off.
Up	Down	Almost always refers to data link layer problems, most often configuration problems. For example, serial links have this combination when one router was configured to use PPP and the other defaults to use HDLC.
Up	Up	Layer 1 and Layer 2 of this interface are functioning.

Figure 36: Interface Statuses

Errdisable

This feature was first implemented to handle special collision situations in which the switch detected **excessive** or **late collisions** on a port. **Excessive collisions** occur when a frame is dropped because the switch encounters **16 collisions in a row**. **Late collisions** occur after every device on the wire should have recognized that the wire was in use.

- By **default**, ports put into the errdisable state must be re-enabled manually

Possible causes of these types of errors include:

- A cable that is out of specification (either too long, the wrong type, or defective)
- A bad network interface card (NIC) card (with physical problems or driver problems)
- A port duplex misconfiguration
 Is a common cause of the errors because of failures to negotiate the speed and duplex properly between two directly connected devices (for example, a NIC that connects to a switch). Only half-duplex connections should ever have collisions in a LAN. Because of the carrier sense multiple access (CSMA) nature of Ethernet, collisions are normal for half duplex, as long as the collisions do not exceed a small percentage of traffic.

There are various reasons for the interface to go into **errdisable**. The reason can be:

- Duplex mismatch
- Port channel misconfiguration
- BPDU guard violation
- UniDirectional Link Detection (UDLD) condition
- Late-collision detection
- Link-flap detection
- Security violation
- Port Aggregation Protocol (PAgP) flap
- Layer 2 Tunneling Protocol (L2TP) guard
- DHCP snooping rate-limit
- Incorrect GBIC / Small Form-Factor Pluggable (SFP) module or cable
- Address Resolution Protocol (ARP) inspection
- Inline power

Configuring ERRDISABLE:

```
(config)#errdisable detect cause all| cause-name
(config)#errdisable recovery interval 60
```

Triggers:

all	Detects every possible cause
arp-inspection	Detects errors with dynamic ARP inspection
bpduguard	Detects when a spanning-tree bridge protocol data unit (BPDU) is received on a port configured for STP PortFast
dhcp-rate-limit	Detects an error with DHCP snooping
dtp-flap	Detects when trunking encapsulation is changing from one type to another
gbic-invalid	Detects the presence of an invalid GBIC or SPF module
inline-power	Detects an error with offering PoE inline power
l2ptguard	Detects an error with Layer 2 Protocol Tunneling
link-flap	Detects when the port link state is "flapping" between the up and down states
loopback	Detects when an interface has been looped back
pagp-flap	Detects when an EtherChannel bundle's ports no longer have consistent configurations
pppoe-ia-rate-limit	Detects errors with PPPoE Intermediate Agent rate limiting
psecure-violation	Detects conditions that trigger port security configured on a port
psp	Detects an error related to protocol storm protection
security-violation	Detects errors related to 802.1X security
sfp-config-mismatch	Detects errors related to SFP configuration mismatches
small-frame	Detects errors when VLAN-tagged packets are too small and arrive above a certain rate
storm-control	Detects when a storm control threshold has been exceeded on a port
udld	Detects when a link is seen to be unidirectional (data passing in only one direction)

PoE - Power over Ethernet

PoE Methods

ILP	Cisco Inline Power
PoE	IEEE 802.3af
PoE+	IEEE 802.3at
UPoE	Cisco Universal PoE

Power Classes

0 (default)	15.4W
1	4.0W
2	7.0W
3	15.4W
4 (802.3at)	Up to 30 W

Configuring PoE

```
(config-if) #power inline auto  
(config-if) #power inline never
```

Troubleshooting PoE

```
#show power inline
```

VIRTUAL LANs (VLANs) and INTER VLAN ROUTING

- VLANs are operating on **OSI-Layer 2**
- Both **collision** and **broadcast domains** can easily be controlled with routers and VLANs.
- By creating VLANs you break up a pure switched internetwork into different **broadcast domains**. A VLAN is treated like its own **subnet** or **broadcast domain**.
A VLAN = A Broadcast Domain = An IP Subnet
- By default, hosts in a specific VLAN can't communicate with hosts that are members of another VLAN.
- **VLAN 1** is the native and management VLAN by default
- The **native VLAN** frames are **not tagged** when transmitted across an 802.1Q Trunk.

- By default, all ports on the switch are in **VLAN 1**
- You may create VLAN 1 - 4094. In fact, only up to 1001
- Special VLANs 1, 1002-1005 they are reserved
- VLAN numbers 1006 - 4094 are called **extended VLANs**
- If the switch is configured as **VTP server** or **client**, the VLAN commands are stored in the **vlan.dat** file in flash.
- Each port that is assigned to a VLAN receives a **PVID**.

PROs:

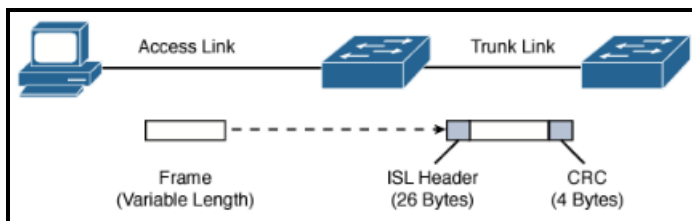
- Improve network performance
- Limit broadcast storms
- Improve adds, moves, and changes
- Minimize security problems
- Ease your management task

Frame Tagging

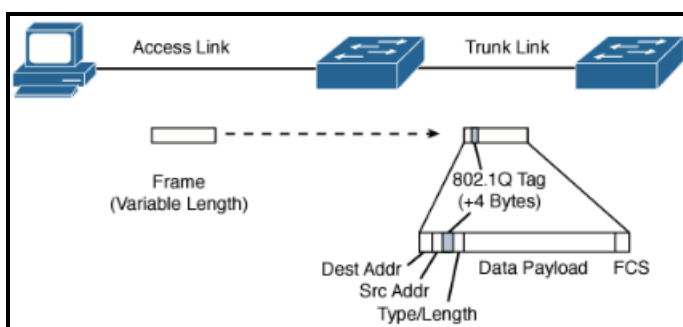
This *frame identification method* uniquely assigns a user-defined VLAN ID to each frame.

VLAN Identification Methods

- **Inter-Switch Link (ISL)**
ISL *encapsulates* the frame with control information.
Even Cisco is moving to use 802.1q instead of ISL.
ISL does not support untagged VLAN



- **IEEE 802.1q**
Supports up to 4094 VLANs.
Inserts a 4 Byte 802.1q field with tag control information.
Uses a native VLAN



VLAN Membership

- Static VLAN configuration
- Dynamic VLAN assignment
Provide membership based on the MAC address of a device.
They require more administrative overhead, since the network administrator must assign the MAC address manually to a VLAN.

Configuring VLANs

0 and 4095	Reserved (--)	For system use only You cannot see or use these VLANs
1	Normal (VTP)	Cisco default . You can use this VLAN but you cannot delete it. Type Ethernet with max. MTU of 1500
2-1001	Normal (VTP)	For Ethernet VLANs You can create, use and delete these VLANs
1002-1005	Normal (VTP)	Cisco defaults for FDDI and Token Ring. You cannot delete VLANs 1002-1005
1006-4096	Extended (No VTP)	For Ethernet VLANs only The mode must be <code>vtp mode transparent</code>

```
(config)#vlan [VID]                → Set VLAN-ID 0-4094
(config)#no vlan [VID]             → Remove VLAN-ID
(config-vlan)#name [VLAN-Name]    → Optional
```

Assign VLANs to Ports

```
(config)#interface [IF]           → int fa0/1
(config-if)#switchport mode access
(config-if)#switchport access vlan [VID]
```

Remove VLAN from Port

```
(config-if)#switchport trunk allowed vlan remove [VID]
```

```
#show vlan
#show vlan brief
#show vlan id [x]
#show interface [IF] switchport
#show interface trunk
```

Configuring Trunk Ports

- Trunk ports send and receive information **from all VLANs by default**
- If a frame is untagged it's sent to the **management VLAN**

```
(config)#int range f0/15-18
(config-if)#switchport
(config-if)#switchport trunk encapsulation dot1q | isl | negotiate
(config-if)#switchport mode trunk
```

Prevent VLANs

```
int f0/15
switchport trunk allowed vlan 4,6,12,15
...
switchport trunk allowed vlan remove 4-8
...
switchport trunk allowed vlan all
```

Change Native VLAN

```
int f0/15
switchport trunk native vlan 4
...
no switchport trunk native vlan
```

Configuring Router on a Stick (ROAS)

1. Switch: Create the necessary VLANs
interface vlan [vlanID]

2. **Switch:** Associate the appropriate access mode
`switchport access vlan [vlanID]`
3. **Switch:**
`(config-if)#switchport mode trunk`
4. **Router:** Create the proper subinterfaces
`interface [fa0/1.10]`
5. **Router:**
`(config-subif)#ip address [ip_address] [network_mask]`
6. **Router:**
`switchport trunk encapsulation dot1q`
`(config-subif)#encapsulation dot1q [vlanID]`

Configuring Inter-VLAN Routing

```
ip routing
interface vlan 10
ip address x.x.x.x m.m.m.m
interface vlan 20
ip address x.x.x.x m.m.m.m
```

Switched Virtual Interface (SVI)

A **Switched Virtual Interface (SVI)** is a VLAN of switch ports represented by one interface to a routing or bridging system. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN.

There is **one-to-one** mapping between a VLAN and SVI, thus only a single SVI can be mapped to a VLAN. By default, an SVI is created for the default VLAN (VLAN1) to permit remote switch administration. An SVI cannot be activated unless associated with a physical port.

SVIs are generally configured for a VLAN for the following reasons:

- Allow traffic to be routed between VLANs by providing a default gateway for the VLAN.
- Provide fallback bridging (if required for non-routable protocols).
- Provide Layer 3 IP connectivity to the switch.
- Support bridging configurations and routing protocol.

SVIs advantages include:

- Much faster than router-on-a-stick, because everything is **hardware-switched** and routed.
- Latency is much lower, because it does not need to leave the switch.
- No need for external links from the switch to the router for routing.
- Not limited to one link. Layer 2 EtherChannels can be used between the switches to get more bandwidth.

An SVI can also be known as a **Routed VLAN Interface (RVI)** by some vendors.

TCAM

Ternary Content Addressable Memory (TCAM).

- Is a type of **memory**.
- Uses **Masks** and **Patterns**.
- Holds only information's which are active.

If you are running out of space for the TCAM, you will get a SYSLOG message.

```
#show tcam counts
#show tcam ina1 size
#show tcam ina1 statistics
```

Configuring SVI

```
(config)#ip routing  
(config)#interface vlan 10  
(config-if)#description SALES  
(config-if)#ip address 10.0.0.1 255.255.255.0  
(config-if)#no shutdown
```

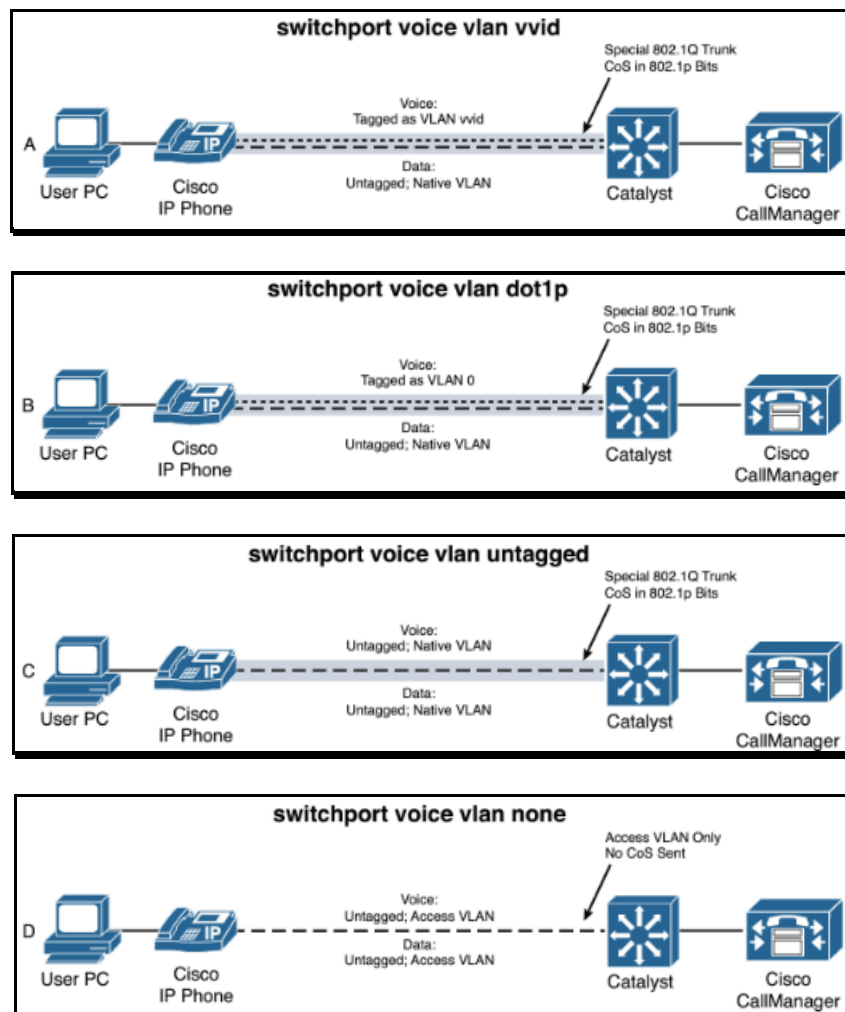
→ Enables IPv4 routing on the switch
→ Creates an SVI for VLAN 10
→ Adds description
→ Assigns IP Address
→

Troubleshooting SVI

```
show ip interface brief →  
show running-config →  
show interface →
```

VoIP - Data and Voice VLANs

- The phone sends voice traffic with Layer 3 IP precedence and Layer 2 **class of service (CoS)** values, which are both set to **5 by default**.
- Because the sound quality of an IP phone call can deteriorate if the data is unevenly sent, the switch supports quality of service (QoS) based on **IEEE 802.1p** CoS.
- You should configure voice VLAN **on switch access ports**; voice VLAN is not supported on trunk ports.
- To verify **one-way packet loss**, you need to enable IP Service Level Agreements (SLA) on a router.
- The **802.1p** value allows you to assign up to **eight different levels of priorities** to the customer traffic.
- **G.114** recommends, that the **one-way latency** for VoIP traffic should not exceed **150 ms**,
- **DHCP option 150** is used to provide a **TFTP server**, where the phone can download the config.
- The voice VLAN is also called **VVID**



Configuring Data and Voice VLAN

For achieving **high sound and video quality**, you should use the following values:

- Delay (one-way): 150 ms
- Jitter: 30 ms
- Loss: 1%

For achieving **high video quality**, you should use the following values:

- Delay (one-way): 200-400 ms
- Jitter: 30-50 ms
- Loss: < 1%
- Bandwidth: >= 384 Kbps

```
(config)#vlan 10
(config-vlan)#name VOICE
(config-vlan)#vlan 50
(config-vlan)#name DATA
```

#udp-jitter

→ See IP SLA

Configure IP Phone

```
(config-if)#switchport voice vlan [VID]
```

```
#show vlan brief
```

```
#show interfaces [x] switchport
```

```
#show ip sla summary
```

Private VLANs (PVLANS)

- Web hosting in an ISP's server farm.
- Isolation between customers.
- Route to the @internet.
- Intra-partition communication.
- Users are in two VLANs (Primary VLAN, Private VLAN)..

Troubleshooting VLAN

```
#show vlan
```

```
#show vlan brief
```

```
#show vlan id [x]
```

```
#show interface status
```

```
#show interface [IF] switchport
```

```
#show interface [IF] trunk
```

```
#show interface trunk
```

→ Shows:

The VLANs allowed on the trunk

The encapsulation method used for the trunk

The interfaces which are trunks

The native VLAN

The administrative mode used to form the trunk

```
show vtp status
```

```
show vtp domain
```

```
show vtp statistics
```

```
show port [x/x]
```

```
show run | include vtp
```

→

```
#show spanning-tree interface [IF]
```

```
#show spanning-tree interface [IF] portfast
```

```
show mac address-table
```

→

```
show mac address-table | include 2b00
```

```
switchport access vlan
```

→


```

Router# show vlan

VLAN Name                Status    Ports
-----
1    default                active    Fa5/9
2    VLAN0002                active    Fa5/9
3    VLAN0003                active    Fa5/9
4    VLAN0004                active    Fa5/9
5    VLAN0005                active    Fa5/9
6    VLAN0006                active    Fa5/9
<...Output truncated...>

1004 fddinet-default        active    Fa5/9
1005 trbrf-default        active    Fa5/9

VLAN Type  SAID      MTU   Parent RingNo BridgeNo Stp   BrdgMode Trans1 Trans2
-----
1    enet     100001   1500  -     -     -     -     -     0     0
2    enet     100002   1500  -     -     -     -     -     0     0
3    enet     100003   1500  -     -     -     -     -     303   0
4    enet     100004   1500  -     -     -     -     -     304   0
5    enet     100005   1500  -     -     -     -     -     305   0
6    enet     100006   1500  -     -     -     -     -     0     0
10   enet     100010   1500  -     -     -     -     -     0     0

<...Output truncated...>

Remote SPAN VLANs
-----
2, 20

Primary Secondary Type          Ports
-----

```

Figure 37: show vlan

```

Router# show vlan brief

VLAN Name                Status    Ports
-----
1    default                active    Fa5/9
2    VLAN0002                active    Fa5/9
3    VLAN0003                act/lshut Fa5/9
4    VLAN0004                act/lshut Fa5/9
5    VLAN0005                active    Fa5/9
10   VLAN0010                active    Fa5/9
.
.
.
999  VLAN0999                active    Fa5/9
1002 fddi-default            active    Fa5/9
1003 trcrf-default        active    Fa5/9
1004 fddinet-default        active    Fa5/9
1005 trbrf-default        active    Fa5/9

```

Figure 38: show vlan brief

```

n1000v(config)# show interface trunk
-----
Port Native Status Port
Vlan Channel
-----
Eth2/9 1 trunking --
Eth2/10 1 trnk-bndl Po50
Po50 1 not-trunking --
-----
Port Vlans Allowed on Trunk
-----
Eth2/9 1-3967,4048-4093
Eth2/10 1-3967,4048-4093
Po50 1-3967,4048-4093
-----
Port STP Forwarding
-----
Eth2/9 none
Eth2/10 none
Po50 none

```

Figure 39: show interface trunk

Administrative Modes

- Cisco routers do not talk **Dynamic Trunk Protocol (DTP)**
- The process of DTP message exchange adds some delay in negotiating and bringing up a trunk. Use '**switchport mode trunk**' + '**switchport nonegotiate**' + '**switchport trunk encapsulation**' for the fastest possible formation of a trunk.
- DTP sends data on **VLAN 1**
- **DTP frames** are sent out **every 30 seconds** to keep neighboring switch ports informed of the link's mode.
- **Best Practise:** Configure both ends of a trunk link as `switchport mode trunk` OR `switchport mode access`.

- **switchport nonegotiate**
Do not send or respond to DTP from this end. Disable all DTP on this port (Best used on user access ports, when trunking to non-Cisco switches, when trunking to a router, or if you are paranoid about fast convergence)
- **switchport mode access**
unconditional
Never trunk on this end, and I will send out DTP to help my link partner reach the same conclusion.
- **switchport mode dynamic desirable**
Actively initiate negotiation
Ask the other end to trunk using DTP and trunk if the negotiation succeeds. If DTP negotiation fails then become an access port.
- **switchport mode dynamic auto** (DTP Default)
Passively negotiate (but not actively)
If the other end asks me to be a trunk with DTP, then become a trunk, but I won't initiate any negotiation from this end. If no one asks me to become a trunk then I will become an access port.
- **switchport mode trunk**
unconditional
Always trunk on this end, and I will send DTP to attempt to negotiate a trunk on the other end.

- **switchport trunk encapsulation**

unconditional

Do not negotiate the trunk protocol with DTP. Only use the trunk protocol specified in this command (isl or dot1q).

Matrix erstellen!!!

Nonegotiate

Access

Dynamic desirable

Dynamic auto

Trunk

Encapsulation

Which of the following switch port modes will successfully form a trunk between two switches?
(Choose four)

- A. Dynamic desirable – dynamic auto
- B. Trunk – dynamic desirable
- C. Access – dynamic auto
- D. Trunk - trunk
- E. Dynamic auto – dynamic auto
- F. Trunk – access
- G. Trunk – dynamic auto

Operational Modes (Actual status)

down

→

trunk

→ Trunk mode

static access

→ Access mode

VLAN Trunk Protocol (VTP)

- Cisco proprietary **Layer 2** protocol.
- To manage VLANs from a **central point of control**.
- VLAN Trunk Protocol (VTP) reduces administration in a switched network.
- When you configure a new VLAN on one **VTP server**, the VLAN is distributed through all switches in this domain. This reduces the need to configure the same VLAN everywhere.
- VTP is a Cisco-proprietary protocol that is available on most of the Cisco Catalyst series products.
- VTP creates by default **broadcast traffic** for all switches. You may reduce this by using **VTP pruning**
- You need to allocate a **VTP Domain** and the **VTP version** must match.
- You may create **VTP passwords**.
- The highest **VTP Configuration Revision Number** is the most recent.
- VTP advertisements are sent as **multicast frames**.

There are 3 types of advertisements:

- Summary advertisements
- Subset advertisements
- Advertisement requests from clients

VTP versions

- The same VTP version should be configured on every switch in a management domain.
- **Version 1**
VLAN 1 to 1005
- **Version 2**
VLAN 1 to 1005

- **Version 3**
VLAN 1 to 4094

VTP Domains

- VTP is organized into **management domains**.
- A switch can belong to only **one (1) domain**.
- A VTP domain must have at least one **server**.

VTP Modes

- **Server Mode** In VTP server mode, you can create, modify, and delete VLANs and specify other onfiguration parameters, such as VTP version and VTP pruning, for the entire VTP domain. VTP servers advertise their VLAN configuration to other switches in the same VTP domain and synchronize their VLAN configuration with other switches based on advertisements received over trunk links. VTP server is the **default mode**.
- **Client Mode** VTP clients behave the same way as VTP servers, but you **cannot create, change, or delete** VLANs on a VTP client.
The local VLAN configuration is updated only when an update that has a higher **configuration revision number** is received.
After reboot they send a **VTP advertisement request** to the VTP servers.
The switches act as **VTP relay**.
This is a **passive listening mode**.
- **Transparent Mode** VTP transparent switches do not participate in VTP. A VTP transparent switch **does not advertise** its VLAN configuration and does not synchronize its VLAN configuration based on received advertisements, but transparent switches do forward VTP advertisements that they receive out their trunk ports in VTP Version 2. The **configuration revision number** will always be 0 (zero).
Manual adding/deleting VLANs allowed.
- **Off Mode** (configurable only in CatOS switches)—In the three described modes, VTP advertisements are received and transmitted as soon as the switch enters the management domain state. In the VTP off mode, switches behave the **same as in VTP transparent mode** with the exception that VTP advertisements are not forwarded

VTP Pruning

- Preserves bandwidth by reducing the amount of broadcast, multicast and unicast packets.
- Broadcast, multicast and unknown unicast frames on a VLAN are forwarded over a trunk link only if the switch on the receiving end of the trunk has ports in that VLAN.
- By default, VTP pruning is **disabled**.
- VTP pruning has no effect on switches in the **VTP transparent mode**.
- **VLAN 1** is never eligible for pruning.
- **VLAN 1002 - 1005** are reserved for Token Ring and FDDI VLANs and are never eligible for pruning.

```
(config)#vtp pruning
(config-if)#switchport trunk pruning vlan 3-4
```

switchport trunk allowed vlan

Configure VTP database mode

Note: If a switch is configured as a **VTP server** without a **VTP domain name**, you cannot configure a VLAN on the switch.

Configure VTP database mode

```
#vlan database
(vlan)#vtp domain-name          → Set the VTP domain name
(vlan)#vtp client | server | transparent → Set the VTP mode
switchport trunk pruning vlan    →
```

(config)#[no] vtp pruning

→ Reduces

Configure VTP mode

(config)#**vtp mode client | server | transparent | off**

Configure VTP version

(config)#**vtp version 1 | 2 | 3**

switchport mode trunk

Troubleshooting VTP

- Check the VTP Domain name.
- Check the VTP Revision number.
- Assure new added switches have a revision number of 0.
- Is the switch configured for VTP transparent mode?
- Is the link towards the VTP server in trunking mode?

#**show run | include vlan**

#show vtp domain

#**show vtp status**

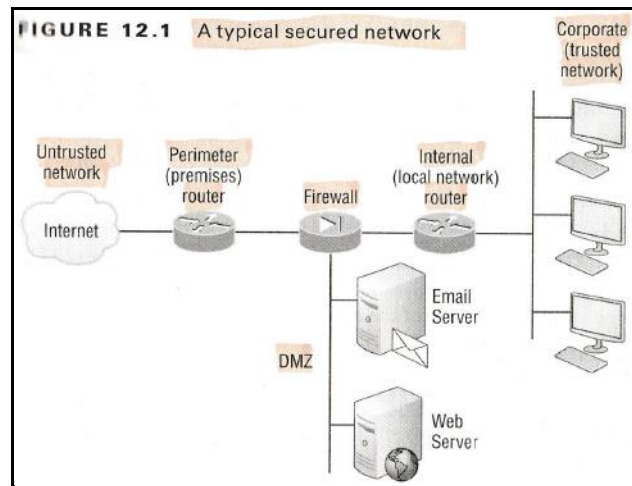
#show run | include vlan

#**show vlan brief**

#show vtp statistics

#**debug dtp packet**

SECURITY



Access Control Lists (ACLs)

- Essentially a list of conditions that **classify** packets.
- **Classification** tool.
- You can assign only one access list per interface per protocol per direction. Means **1 Interface** can have **two ACLs** one inbound and one outbound.
- An ACL performs matching and filtering based on **addressing** information.
- Related/attached to an **object**.

Hint: Ping and traceroute are working properly, but other protocol connections fail. This can be an indication, that ACL is filtering traffic.

1. Packets are processed sequentially through the access list
2. If a match is made, **no further condition** is checked
3. At the end is an **implicit "deny"** and packets with no match will be discarded
4. To define ranges, you need **wildcard masking**

General Rules

- Organize your access lists so that the more specific tests are at the top
- Use a text editor to manage the access list

Rules: Traffic from the @Internet to your production network

- Deny any source addresses from your internal networks
- Deny any local host addresses (127.0.0.0/8)
- Deny any reserved private addresses (RFC 1918)
- Deny any addresses in the IP multicast range (224.0.0.0/4)

Security threats you can mitigate with ACLs:

- IP address spoofing, inbound and outbound
- Denial of service (DoS) TCP SYN attacks, blocking external attacks
- DoS TCP SYN attacks, using TCP intercept
- DoS smurf attacks
- Denying/Filtering ICMP messages, inbound and outbound
- Denying/Filtering Traceroute
- Accessing routers with Telnet or SSH (see access-class)

Router Access Control Lists (RACLs)

- To control traffic from one subnet to another.

VLAN Access Control Lists (VACLs)

- VACLs control access to the VLAN of all packets (bridged and routed).

- You can use VACLs to filter traffic between devices in the same VLAN.
- IGMP packets are not checked against VACLs.
- Also, called **VLAN access-maps**.
- VACLs are not defined by direction (input or output).
- VACLs can be used to **capture** traffic.

Configuring VACL

```
(config)#access-list 101 permit ip host 1.1.1.1 host 2.2.2.2
(config)#vlan access-map VLAN10-VACL
match ip address 101
action drop
```

```
-----
(config-if)#switchport capture
```

Troubleshooting VACL

```
#show vlan access-map [map-name]
#show vlan filter [map-name|vlan id]

#show security acl
#show security acl editbuffer
#show security acl info
#show security acl resource-usage
```

Port Access Control Lists (PACLs)

- PACLs perform access control on all traffic entering the specified Layer 2 port.

Layer 4 Operators (L4 Ops)

- L4 Ops are stored in Logical Operation Units (LOUs).

e.g. access-list 101 permit tcp host 10.1.1.1 host 10.2.2.2 **gt 1023**

- The addition **<gt 1023>** applied to an ACL adds a <Layer 4 Operator>

Standard access lists

- Decisions will be taken based on the **source IP address**.
- By using numbers **1-99** or **1300-1999**, you are telling the router that you want to create a standard IP access list.
- Applied closest to the destination!

```
access-list [0-99 | 1300-1999] [permit | deny] [matching parameters] [log]
```

```
access-list 1 permit host 10.1.1.1 → (host) Obsolete
```

```
access-list 1 permit 10.1.1.1
access-list 1 permit 10.1.1.0 0.0.0.255
access-list 1 permit any
access-list 1 permit any log
ip access-group 1 [in | out]
```

Extended access lists

- They can evaluate many of the **other fields** in the layer 3 and layer 4 traffic
- Use access-list range **100 - 199** or **2000-2699**
- Applied closest to the source!
- If the **log** keyword is used packets will be matched **process switched**.

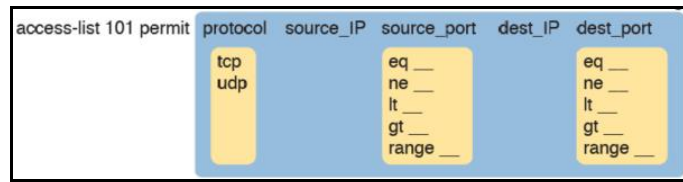


Figure 40: Extended ACL

Fields to be compared in the extended ACL

- Source IP address
- Protocol
- Destination IP Address
- ToS byte (QoS)

```
access-list [100-199|2000-2699] [permit|deny] [prot] [src-ip/wc] [port] [dst-ip/wc] [port] [log]
```

Named access lists

They are either **Standard** or **Extended**.

```
(config)#ip access-list extended BLOCK_UDP
(config-ext-nacl)#deny udp any any
(config-ext-nacl)#permit ip any any
```

Time-Based ACLs

```
(config)#time-range [NAME]
(config-time-range)#periodic weekdays 8:00 to 17:00
(config)#access-list 100 permit tcp any host [IP] eq 80 time-range [NAME]
```

Periodic

- Specifies a recurring time period for which the time range is valid.

```
(config-time-range)#periodic Monday 8:00 to 17:00
...
(config-time-range)#periodic Sunday 8:00 to 17:00
```

Absolute

- Specifies a single time period for which the time range is valid; you can specify a beginning time, an ending time, or both.

```
absolute [start] [end]
```

Infrastructure ACLs

- Typically, an extended ACL applied to an internet facing router.
- Target, to prevent malicious traffic from entering the enterprise.
- Take care of **UDP port 1701 / L2TP**.
- Take care of **IP Protocol number 50 / ESP**.

```
(config)#ip access-list extended INFRASTRUCTURE
```

Context-Based ACLs (CBAC)

- The **Cisco IOS Firewall** feature must be set.

```
(config)#ip inspect name [X] [protocol] timeout [sec]
```

Configure ACLs

```
(config-ext-nacl)#access-list 100 deny udp any any
```

Should be the last statement in an access-list to eliminate the implicit deny.

```
(config-ext-nacl)#access-list 100 permit ip any any
```

Block Packet Fragments

```
(config-ext-nacl)#deny tcp any any fragments
(config-ext-nacl)#deny udp any any fragments
(config-ext-nacl)#deny icmp any any fragments
(config-ext-nacl)#deny ip any any fragments
```

Prevent DOS attacks with option Fragments

```
(config-ext-nacl)#deny tcp any INFRASTRUCTURE_IP fragments
```

Allow Necessary Routing Protocols and Network Management Traffic

```
(config-ext-nacl)#permit tcp host [ext-bgp-peer] host [int-bgp-peer] eq bgp
(config-ext-nacl)#permit tcp host [ext-bgp-peer] eq bgp host [int-bgp-peer]
(config-ext-nacl)#permit tcp [IP-Mgmt-station] any eq 22
(config-ext-nacl)#permit tcp [IP-Mgmt-station] any eq 161
(config-ext-nacl)#permit icmp [IP-Mgmt-station] any echo
```

Block all Other Traffic to INTRANET

```
(config-ext-nacl)#deny ip any [Space-Intranet]
```

Permit Transit BGP

```
(config-ext-nacl)#permit ip any any
```

Permit Transit BGP

```
(config-ext-nacl)#permit ip any any
```

Apply ACL

```
int s0/0
ip access-group INFRASTRUCTURE in
```

Troubleshooting ACLs

```
show access-list
show access-list 110
show ip access-list
show ip interface [IF]
show running-config
#show tcam counts
```

```
(config)#mls aclmerge algorithm odm
```

```
#debug ip packet [ACL-No]
#debug ip policy
```

NAT - NETWORK ADDRESS TRANSLATION

- **NAT reduces the need for public IPv4 addresses** to only a few addresses per enterprise because of how NAT can multiplex flows using different TCP or UDP port numbers.
- NAT is typically used on a **border router**.
- Cisco's default translation timeout is 86'400 seconds (24 hours).
- Applications requiring **end-to-end connectivity**, where source and destination IP addresses are not modified at any point on the data path, could fail because of NAT's modification of source and destination IP addresses.
- NAT might have compatibility issues with **IPsec**, because IPsec performs message integrity checks, which could fail because of NAT's manipulation of packet header contents.
- There are versions of NAT proxies designed to support IPsec. **NAT-Traversal** (RFC 3947) was designed to support IPsec VPNs using UDP encapsulation of **IKE**.
- In a **Public Key Infrastructure (PKI)** environment, digital certificates can be used for authentication and encryption. However, the digital signature on a digital certificate could be incorrect, based on a device's IP being changed by NAT.

Types of Network Address Translation

Static NAT (SNAT, 1:1)

- Allows one-to-one mapping between local and global addresses
- Requires on public IP address for each host
- Example if you want an email server to be located by other email servers from the @Internet.

```
ip nat inside          → For the NAT inside interface
ip nat outside         → For the NAT outside interface
ip nat inside source static [private IP1] [public IP1]
...
ip nat inside source static [private IPx] [public IPx]
```

Dynamic NAT (DNAT, 1:1)

- Because dynamic NAT don't use port numbers, we must have real IP addresses for every user who's trying to get outside the local network.
- DNAT occurs when inside local addresses (private) are automatically assigned an inside global address (public) from a pool of available addresses.

```
ip nat inside          → For the NAT inside interface
ip nat outside         → For the NAT outside interface
ip nat pool
ip nat pool [MyPool] [IP-Start] [IP-End] netmask [mask]
access-list 1 permit 172.16.0.0 0.0.255.255
ip nat inside source list 1 pool [MyPool]
```

NAT Overload / Port Address Translation (PAT, N:1)

- Is a form of **dynamic NAT**, that maps multiple unregistered IP addresses to a single registered IP address (many-to-one) by using different source ports.
- It's also known as port address translation (**PAT**).
- It permits thousands of users to connect to the @Internet using only **one real global IP address**.
- It lacks on **end-to-end visibility** and can block some applications.
- It can disrupt **stateless protocols**.
- It makes **tunneling** more complex.

```
ip nat inside          → For the NAT inside interface
ip nat outside         → For the NAT outside interface
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface s0/0/0 overload

ip nat inside source list 1 pool [x] overload
```

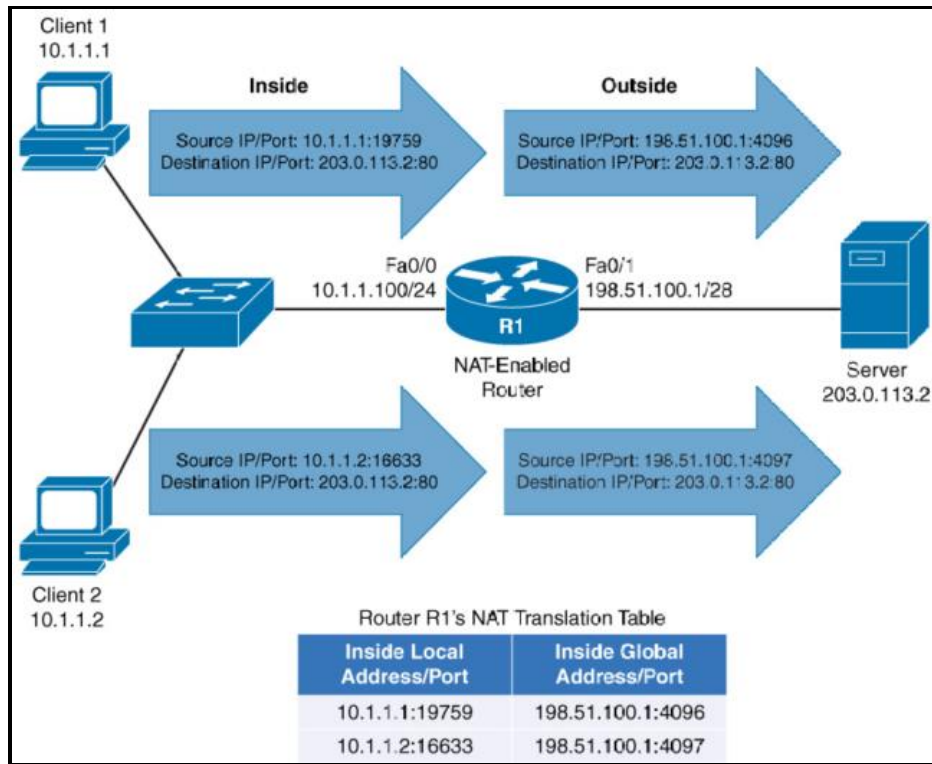
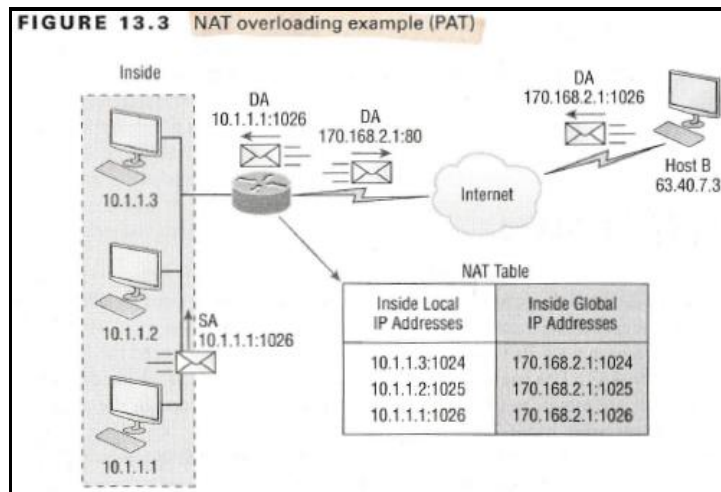


Figure 41: PAT Topology



NAT Virtual Interface (NVI)

Cisco IOS Release >= 12.3

- Can be used with **DNAT** and **PAT** but not with **SNAT**
- No need to define the **inside** or **outside interface**.
- Not all **Cisco IOS** version support NVI.
- NVI makes an **initial routing decision** before performing address translation.
- The resulting virtual interface is called **NVI0**.

```
(config-if)#ip nat enable → For the NAT inside and outside interface
access-list 1 permit 192.168.1.0 0.0.0.255
ip nat inside source list 1 interface Fa0/1 overload
```

```
#show ip nat nvi translations → View the active NAT NVI translations
#show ip nat nvi statistics → View the active NAT NVI statistics
```

Basic NAT

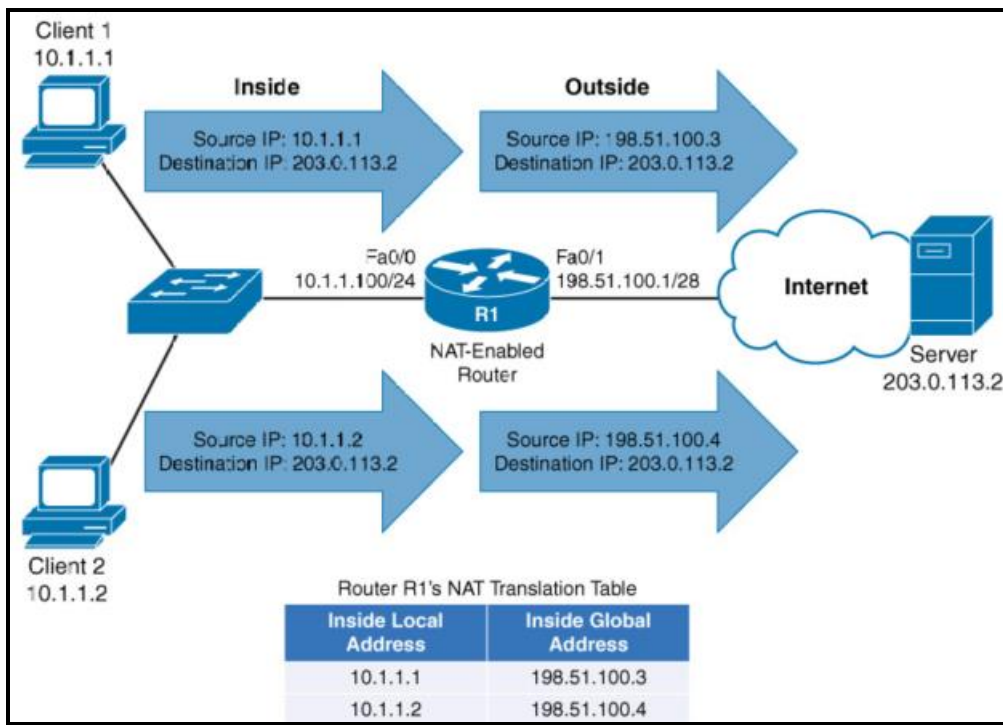
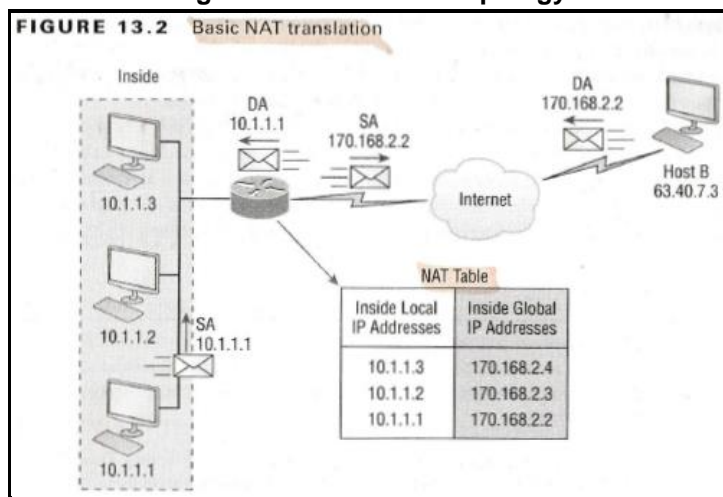


Figure 42: Basic NAT Topology



NAT Names

Inside local	A <u>private IP</u> address referencing an inside device.
Outside local	A <u>private IP</u> address referencing an outside device
Inside global	A <u>public IP</u> address referencing an inside device
Outside global	A <u>public IP</u> address referencing an outside device

The translation of the *inside local* address is done by the boarder router, using an *NAT Table*.

Configuring NAT

Option EXTENDABLE

- The extendable keyword allows the user to configure several ambiguous static translations, where an ambiguous translation are translations with the same local or global address.
- To allow static NAT mappings of one Inside Local address to multiple Inside Global addresses, the keyword extendable is added to the end of the mapping statements. Example 4-23 shows the NAT configuration for Montego

```
ip nat inside source static tcp [] port [IP] extendable
```

Troubleshooting NAT

#show ip nat translations

debug ip nat

debug ip packet

clear ip nat translation [*]

clear ip nat statistics

ip nat translation max-entries

show ip nat statistics

- Hits
- Misses
- Expired translations
- type
- total addresses
- allocated

show ip route

show log

→ View the active NAT translations

→ Use extended access-list to limit the output

→ Shows counters

→

→

→

→ generic

->

→

@INTERNET PROTOCOL VERSION 6 (IPv6)

- **16 Byte** long address (128 bit).
- There are about **7 billion** people on the world. and there are **4.3 billion** IPv4 addresses available.
- IPv6 doesn't use **broadcast**, it's using **multicast** instead.
- There is a new type of communication used in IPv6 called **anycast**.
- When you run IPv4 and IPv6 on a router, you have what is called "**dual stack**".
- There followings are ways of **dynamic addressing with IPv6**.
- For interoperability, IPv4 addresses use the **last 32 bits** of IPv6 addresses.
- IPv6 has a **smoother hierarchical deployment structure** than IPv4.
- **Colon-Hexadecimal** notation is used.
- **Serial interfaces** do not have a built-in MAC address (bin).
- The **IPv4 TTL** field changed in IPv6 to the **Hop Limit** field.
- **Traffic Class** is used for QoS
- **Flow Label** (20 Bit) is used for special handling by the router.

Stateless Address Auto Configuration (SLAAC)

The client picks their own address based on the prefix being advertised on their connected interface. SLAAC provides only the **IPv6 address** and a **default gateway**.

Stateless DHCPv6 server.

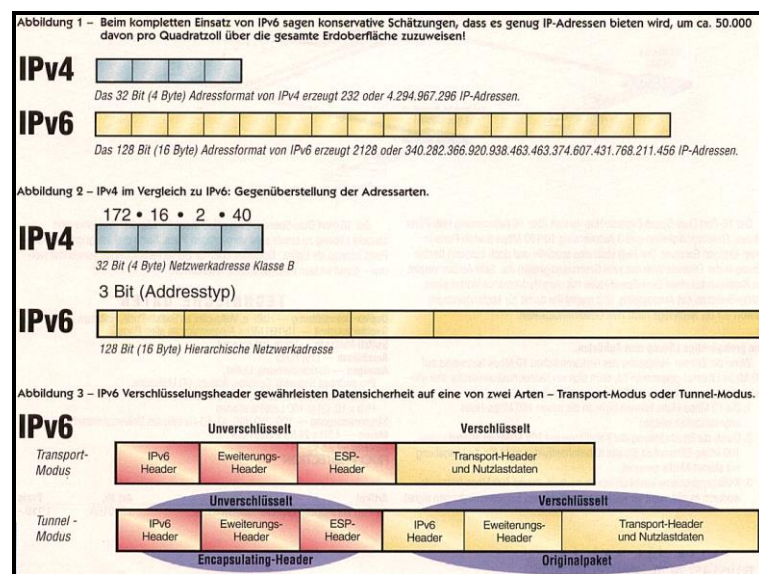
If a router needs more IPv6 information than just an IPv6 address, it might benefit from a stateless DHCPv6 configuration. With this approach, a router obtains an IPv6 address using SLAAC. However, the RA has an **other-config-flag** set, which tells the router to check with a DHCP server to obtain additional IPv6 information such as DNS-Server etc. However,, because the router's IPv6 address was obtained through SLAAC, the DHCPv6 server does not keep track of IPv6 address assignment.

Stateful DHCPv6 (Autoconfiguration uses a DHCPv6 server)

While stateless DHCPv6 allowed a router to obtain an IPv6 address through SLAAC and set the **other-config-flag** instruction the router to learn additional IPv6 configuration information from a DHCPv6 server, Stateful DHCPv6 sets the **managed-config-flag** to instruct the router to obtain its IPv6 address from a DHCPv6 server. Therefore, with Stateful DHCPv6, a DHCPv6 server does keep track of IPv6 address assignment.

DHCPv6 Prefix Delegation (DHCP-v6-PD)

Rather than assigning a single IPv6 address to a router, DHCPv6-PD allows a DHCPv6 server to assign a collection of IPv6 networks to the router. A router could then assign those different IPv6 networks to its various interfaces.



IPv6 fragmentation

- **IPv6 fragmentation** makes it difficult for a firewall to filter fragmented packets.
- **IPv6 fragmentation** works different than IPv4 fragmentation.
- IPv6 uses a **Fragment extension header** for fragmentation.
- In IPv6, the host must fragment UDP packets when the packet is **too big**.
- IPv6 has the no **don't fragment bit**.
- IPv6 router are **dropping packets** which exceed the max MTU size of the outgoing interface.

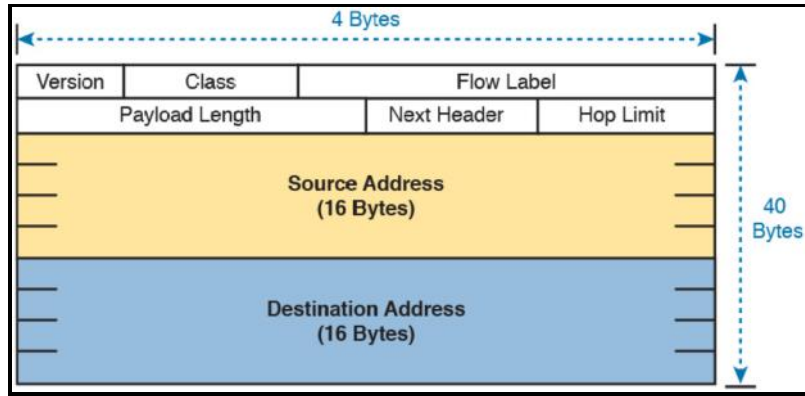


Figure 43: IPv6 Header

IPv6 Naming Conventions

- Omit the leading 0s in any given quartet
- Represent one or more consecutive quartets of all hex 0s with :: but only for one such occurrence in a given address
- IPv6 uses a classless view of addressing, with no concept of classful addressing.
- IPv6 prefixes are often called IPv6 subnets.

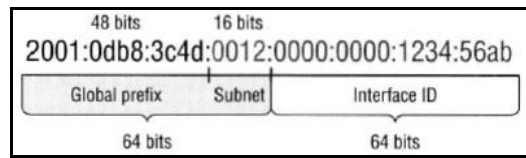


Figure 44: IPv6 Address example

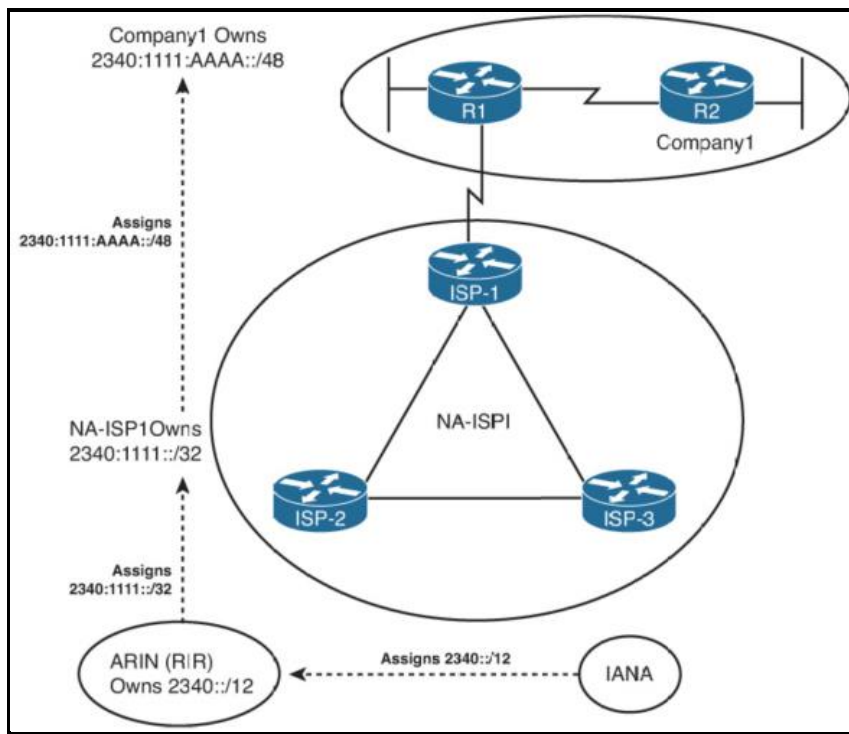


Figure 45: IPv6 Prefix assignment in the @Internet

Connection to a IPv6 web server:

[http://\[2001:::\]/default.html](http://[2001:::]/default.html)

Address	Meaning
0:0:0:0:0:0:0	Equals ::. This is the equivalent of IPv4's 0.0.0.0 and is typically the source address of a host before the host receives an IP address when you're using DHCP-driven stateful configuration.
0:0:0:0:0:0:1	Equals ::1. The equivalent of 127.0.0.1 in IPv4.
0:0:0:0:0:192.168.100.1	This is how an IPv4 address would be written in a mixed IPv6/IPv4 network environment.
2000::/3	The global unicast address range.
FC00::/7	The unique local unicast range.
FE80::/10	The link-local unicast range.
FF00::/8	The multicast range.
3FFF:FFFF::/32	Reserved for examples and documentation.
2001:0DB8::/32	Also reserved for examples and documentation.
2002::/16	Used with 6-to-4 tunneling, which is an IPv4-to-IPv6 transition system. The structure allows IPv6 packets to be transmitted over an IPv4 network without the need to configure explicit tunnels.

See: www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml

- 2000::/3** Global Unicast Address
- 2001:DB8::8:800:200C:417A** Global Unicast Address
- 2002::...** 6to4 Tunnels
- FE80::/10** Link-local Unicast Addresses

	<ul style="list-style-type: none"> - Packets sent in the local subnet - Used as the source for RS and RA messages - Used by Neighbor Discovery (NDP) - Used as the next-hop IPv6 address for IP routes - All addresses beginning with FE8, FE9, FEA or FEB
FEC0::/10	Site Local Unicast
FF01::101	Multicast Address
FF02::1	Multicast Address <ul style="list-style-type: none"> - All IPv6 nodes on the link - NDP router Advertisement - Equivalent to IPv4 subnet broadcast address
FF02::1:2	Multicast Address <ul style="list-style-type: none"> - All routers acting as DHCPv6 relay agent
FF02::2	Multicast Address <ul style="list-style-type: none"> - RS message only received and processed by routers. - All IPv6 routers on the link
FF02::5 / FF02::6	Multicast Address <ul style="list-style-type: none"> - OSPFv3 messages
FF02::9	Multicast Address <ul style="list-style-type: none"> - RIPv2 (RIPng) messages - Used by hosts to send packets to an unknown DHCP server.
FF02::A	Multicast Address (IPv6) <ul style="list-style-type: none"> - EIGRPv6 messages
FF05::1:3	Multicast Address <ul style="list-style-type: none"> - DHCP servers (site scope)
FF05::101	Multicast Address <ul style="list-style-type: none"> - All NTP servers (site scope)
FF08::/16	Multicast Address Used to find DHCP servers
FD00::/8	Unique Local Address <ul style="list-style-type: none"> - Unicast packets inside one organization
FC00::/7	Unique local unicast address <ul style="list-style-type: none"> - Includes all addresses that begin with hex FC and FD
::1	IPv6 Loopback Address <ul style="list-style-type: none"> - Used for software testing - Equivalent to IPv4 127.0.0.1
::	Unspecified Address
/16	Typically assigned to RIRs
/32	Typically assigned to ISPs
/48	Typically assigned to Companies. Global Routing Prefix / Site Prefix

Global Unicast Address (2001:....)

- Packets addressed to a unicast address are delivered to a single interface.
- The communication is **one-to-one**
- **2001::/16** assigned to ARIN (RIR for North America)

Configure a global unicast address

`(config)#ipv6 address 2001::12:1/64` → Assigns a static global address

Configure a global IPv6 address with autoconfigured IP address

`(config-if)#ipv6 address 2001:db8:1:1::/64 eui-64` →

Global unicast address (2000::/3)

- These are your typical **publicly routable addresses**.
- The ISP can provide you with a minimum /48 network ID, which in turn provides you 16-bits to create a unique 64-bit router interface address.
- The last 64-bits are the **unique host ID**.

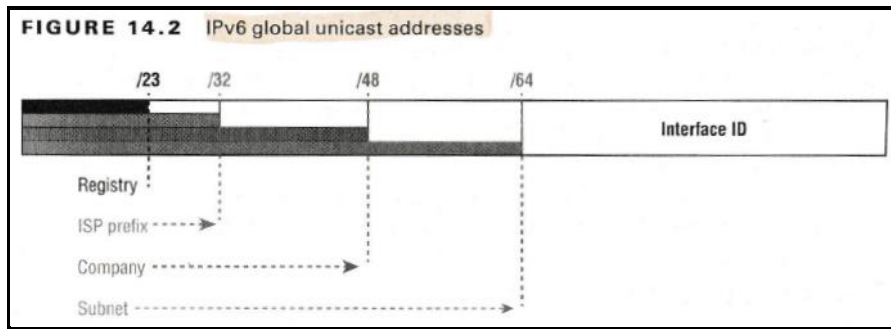


Figure 46: IPv6 Global Unicast Address

Method	Dynamic or Static	Prefix and Length Learned from...	Host Learned from...	Default Router Learned from...	DNS Addresses Learned from...
Stateful DHCP	Dynamic	DHCP Server	DHCP Server	Router, using NDP	(Stateful) DHCP Server
Stateless Autoconfig	Dynamic	Router, using NDP	Derived from MAC	Router, using NDP	Stateless DHCP
Static Configuration	Static	Local config	Local config	Router, using NDP	Stateless DHCP
Static Config with EUI-64	Static	Local config	Derived from MAC	Router, using NDP	Stateless DHCP

Figure 47: IPv6 Address Assignment

Link-local Addresses (FE80::/10)

- These are like the Automatic Private IP Address (APIPA).
- They will **not be routed** in the @Internet.
- Packets to a link-local address **do not leave the IPv6 subnet** because routers do not forward packets sent to a link-local address.
- **All** IPv6 enabled interfaces have a link-local address
- A link-local address is tied to a physical interface

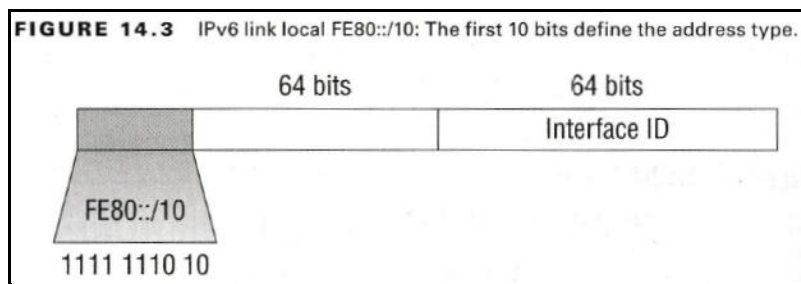


Figure 48: Link Local FE80::/10

Configure a static link-local address

`ipv6 address fe80::12:1 link-local` → Assigns a static link-local address

Unique Local Address (FC00::/7)

- These addresses are also intended for **nonrouting** purposes over the @Internet.

- It has a **well-known prefix** to allow for easy filtering at site boundaries.

Multicast (FF00::/8)

- Sent to all interfaces.
- One host sends a single message to a specific group of users in multicast group. It is a communication between a single host and multiple receivers.

Anycast

- **IPv6** specific
- Addresses identifies **multiple interfaces** on **multiple devices**.
- Packets delivered to anycast addresses as the destination address are delivered to the **nearest interface** identified by that address. Anycast is a communication between a single sender and one of a list of devices with the anycast address.
- **One-to-nearest** communication
- Anycast addresses are typically only configured **on routers**, never hosts and a source address could never be an anycast address. IETF reserved the **top 128 addresses** for **each /64** for use with anycast addresses.

Manual Address Assignment

There are two options for static configuration of IPv6 addresses:

- You configure the entire 128-bit IPv6 address
- You configure the 64-bit prefix and tell the device to use an EUI-64 calculation for the interface ID portion of the address.

The host does not need to statically configure the **default gateway** or the **DNS servers**. The host uses **NDP** to find the **default routers** and **stateless DHCP** to discover the **DNS addresses**.

```
(config)#ipv6 unicast-routing           → Enables IPv6 on the router
ipv6 address 2001:db8:3c4d:1:0260:d6FF:FE73:1987/64
ipv6 address 2001:db8:3c4d:1::/64 eui-64
ipv6 enable                             → Enables Automatic link-local address
```

Solicited Node Multicast address (FF02::1:FF00:0/104)

- A Solicited-Node multicast address is an IPv6 multicast address valid within the local-link (e.g. an Ethernet segment or a Frame Relay cloud). Every IPv6 host will have at least one such address per interface. Solicited-Node multicast addresses are used in **Neighbor Discovery Protocol** for obtaining the layer 2 link-layer addresses of other nodes.
- A Solicited-Node multicast address is created by taking the **last 24 bits** of a unicast or anycast address and appending them to the prefix `ff02::1:ff00:0/104`. It is important to realize that we have taken **104 bits** from the address, so that the last byte of the penultimate field `00` is not used in the prefix. Look at the examples below where the last 24 bits of the multicast address begin after `ff`.
- A host is required to join a Solicited-Node multicast group for each of its configured unicast or anycast addresses.
- In general the solicited-node multicast address is **FF02::1FFXX:XXXX** where the **XX:XXXX** is the right-most 24 bits of the corresponding unicast or anycast address of the interface.

Example: If we have an interface with the IP address `fe80::2aa:ff:fe28:9c5a` the associated Solicited-Node multicast address is `ff02::1:ff28:9c5a`. So we must join to the multicast group represented by this address.

SLAAC - Stateless Address Auto Configuration

- Also, called **Stateless Autoconfiguration (eui-64)**
- **Dynamic** allocation of IP addresses.
- Uses the **64-Bit Prefix** to create the unique address.
- **SLAAC** does not require a server to assign or lease the IPv6 address, does not require the IT staff to preconfigure data per subnet, and does not require the server to track which device uses which IPv6 address.

- Learns the IPv6 prefix used on the link, from any router using **NDP RS/RA** messages.
- Supplies the **DNS servers** IPv6 address to clients.

Uses the following functions:

- Step 1:** IPv6 NDP, particularly the router solicitation and router advertisement messages, to learn the prefix length, and default router.
- Step 2:** Some math to derive the interface ID (host ID) portion of the IPv6 address using a format called EUI-64
- Step 3:** Stateless DHCP to learn the DNS IPv6 address

Configuring SLAAC

```

ipv6 dhcp pool IPV6_POOL
dns-server 2001:1::1
domain-name test.com

interface FastEthernet0/0
ipv6 address 2001:1::1/64
ipv6 enable
ipv6 dhcp server IPV6_POOL

```

```

ipv6 address autoconfig

```

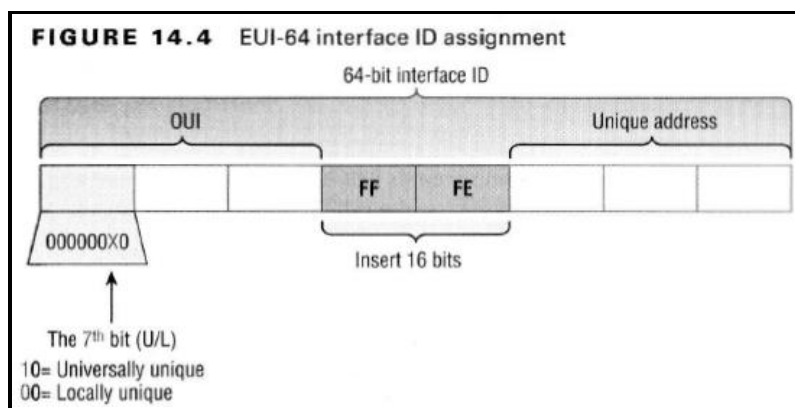
→ Router uses stateless autoconfig to find an address

Modified Extended Unique Identifier (EUI-64) Method

- The interface ID in a IPv6 address is **64 bits** long whereby the MAC address is only 48 bits long, therefore padding with **FFFE** is required to build the interface ID.
- The **interface ID** is caught from the MAC-Address. Whereby the 64-bit interface ID of IPv6 is **padded** with **FFFE**.

e.g. MAC: 0060:d673:1987
 IPv6 Interface ID: 0260:d6**FF:FE**73:1987

The difference of the 7th bit is always **two(2)**.



U/L bit (7th bit)

On the burned in MAC address, the 7th bit is 0(zero)

1. **Router solicitation (RS)** to FF02::2 by using ICMP type 133
2. **Router advertisement (RA)** to multicast FF02::1 by using ICMP type 134

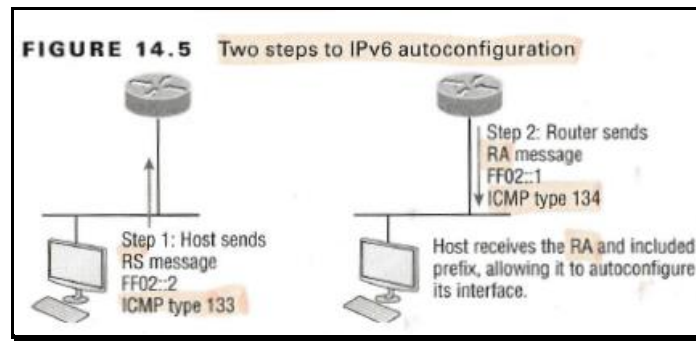


Figure 49: IPv6 Stateless Autoconfiguration

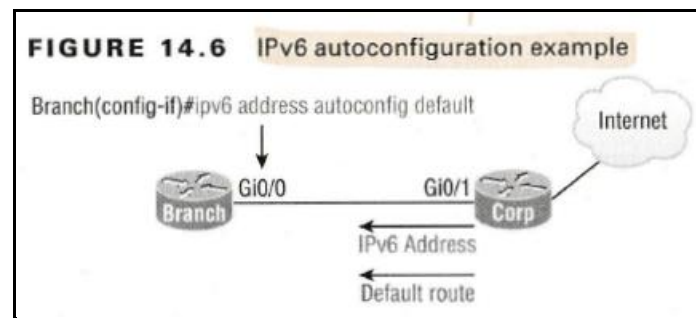


Figure 50: ipv6 address autoconfig default

DHCPv6 (Stateful Dynamic Addressing)

- Stateful DHCP for IPv6
- **Dynamic** address allocation.
- In IPv6 the **RS/RA** process happens first.
- The **RA** that comes back to the client will tell it if DHCP is available for use.
- There is no option for **DNS-Servers**, **domain names**, **default gateway** and **SIP servers**. For this you need another server.
- DHCPv6 does not supply the default router information. **NDP** is used for this.
- **Stateful DHCPv6** servers fill the same role as the older DHCPv4 servers.
- DHCPv4 uses **broadcast** to find the DHCP servers whereas DHCPv6 uses **multicast**.
- The client sends a msg type **1=Solicit** and receives a **type 7=Reply**.

```
ipv6 dhcp server [pool] rapid-commit → Messages: (1) Solicite / (7) Reply
```

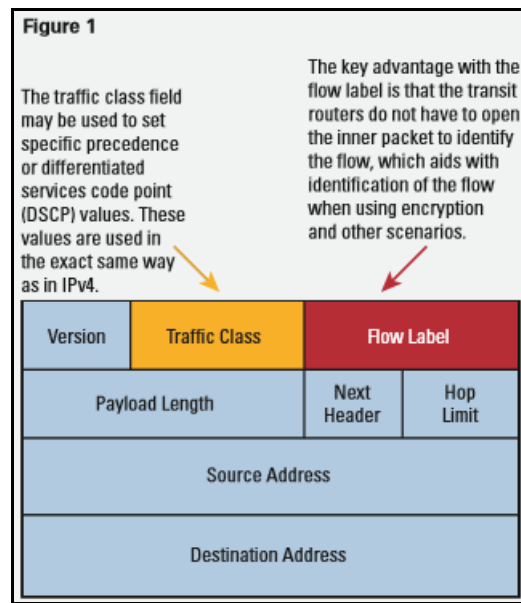
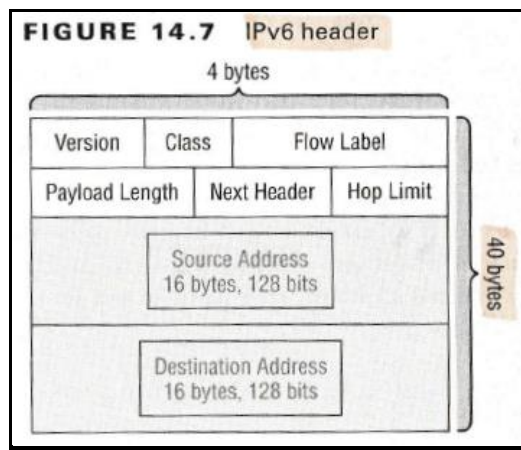
```
(config-if)#ipv6 dhcp relay destination [IPv6] [IF]
```

```
ipv6 address dhcp → Router uses Stateful DHCP to find an address
```

```
#show ipv6 dhcp interface →
```

IPv6 Header

Length = 40 Bytes



ICMPv6

- ICMPv6 has evolved to become **part of the IPv6 packet itself**.
- It doesn't use a **separate layer 3 protocol** and it prevents IPv6 from doing any fragmentation through path MTU discovery.
- ICMPv6 is identified by the value (protocol number) **58** in the **Next Header** field.
- ICMPv6 is used for **router solicitation** and **advertisement**, for **neighbor solicitation** and **advertisement** and for **redirecting** the host to the best router (default gateway).
- ICMPv6 also takes over the task of **finding the address of other devices** on the local link.
- The **IGMP** function of IPv4 is replaced by ICMPv6 and is called the **multicast listener discovery**.

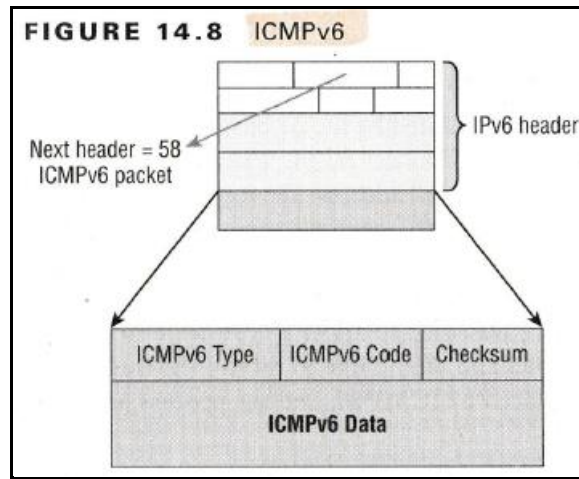


Figure 51: ICMPv6

Neighbor Discovery (NDP)

ICMPv6 also takes over the task of finding the address of other devices on the local link.

- With NDP, the word **neighbor** refers to the fact that the devices will be on the **same data link**. For example, the same VLAN.
- Determining the **MAC address of neighbors**
- **RS/RA** are gathering information about **routers**.
- Router solicitation (**RS**) **FF02::2**
- Router advertisements (**RA**) **FF02::1**
Delivers: Routers IPv6 Address and the Prefix of the link
- Neighbor solicitation (**NS**)
- Neighbor advertisement (**NA**)
- Duplicate address detection (**DAD**)

When the address **FF02:0:0:0:1:FF/104** is queried, the corresponding host will send back its layer 2 address.

NDP NS/NA

- **NS/NA** are gathering information's about **hosts**.

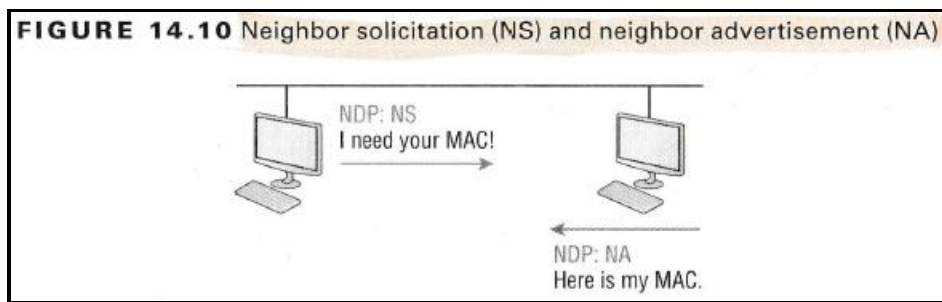


Figure 52: Neighbor Solicitation (NS/NA)

Neighbor Solicitation (NS)

- This message asks a host with a IPv6 address to send back an NA.

Neighbor Advertisement (NA)

NDP RS/RA

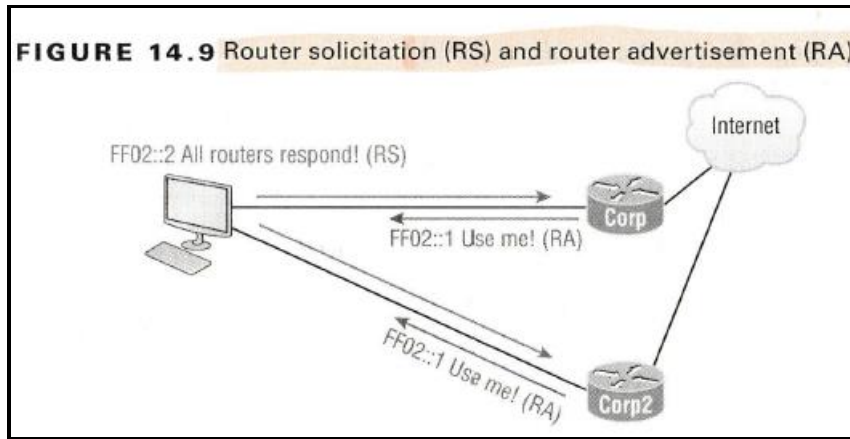


Figure 53: Router Solicitation RS/RA

Router Solicitation (RS)

Router Advertisement (RA)

- RAs are sent out IPv6 interfaces periodically.
- RAs are also sent out when a device solicitation message is sent by a host at system startup.

RA message contains:

- One or more IPv6 prefixes that can be used on the local link to configure their IPv6 addresses.
- The lifetime of each prefix advertised.
- Flags that identify whether **Stateless** or **Stateful** autoconfiguration is permitted.
- Information about the default device that should be used.
- Information related to the maximum transmission unit (MTU) and hop limit that the clients need to apply to packets that they create.
- **SLAAC** clients receive their addressing information's solely from RAs.

Duplicate Address Detection (DAD)

When an IPv6 interface first learns an IPv6 address, or when the interface begins working after being down for any reason, the interface performs Duplicate Address Detection (DAD). The purpose is to prevent duplicate address conflicts.

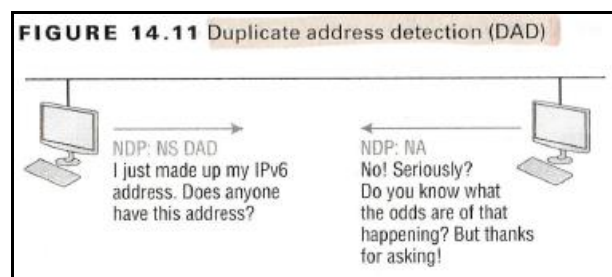


Figure 54: Duplicate Address Detection (DAD)

Inverse Neighbor Discovery (IND)

- IPv6 solves the discovery problem on LANs using Reverse ARP.
- IPv6 solves the problem using Inverse Neighbor Discovery (IND).
- Using Inverse NS (INS) and Inverse NA (INA)

IPv6 Routing Protocols

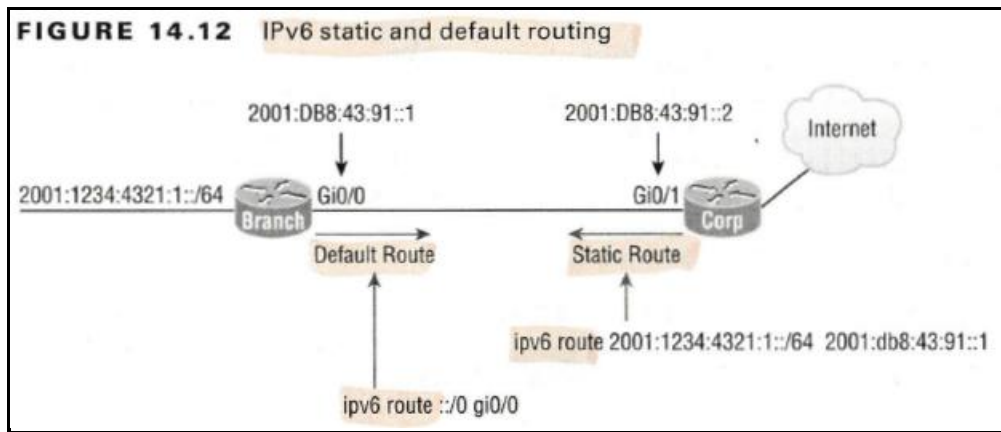
- IPv6 RIPng (next generation)
- EIGRPv6
- OSPFv3

Static Routing with IPv6

```
ipv6 route 2001:db8:3c4d:14::/64 2001:db8:3c4d:12:21a:2fff:fee7:4398 150
```

```
ipv6 route 2001:db8:3c4d:15::/64 s0/1 150
```

```
show ipv6 route static
```



Transition Strategies

- NAT-PT
- 6to4 Tunneling
- Dual Stacking

6to4 Tunneling

RFC 3056

- Connection of **native IPv6** Domains via IPv4 Clouds.
- **Transition tool**, not a permanent solution.
- Also, called "**Dual-Stack-Routers**" or "**6to4 Gateways**"
- The network prefix starts always with **2002:...**

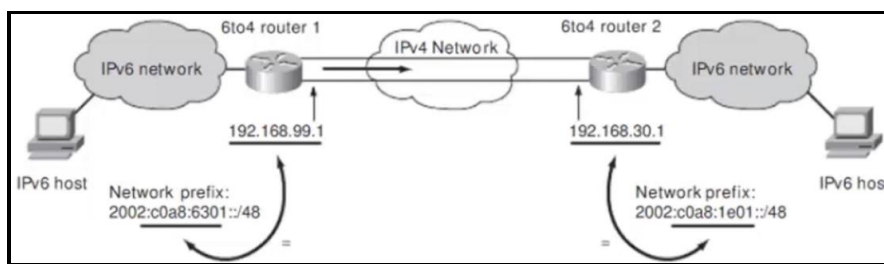


Figure 55: 6to4 Tunnel

Configuring 6to4 Tunnel

```
(config)#ipv6 unicast-routing
interface Tunnel0
ipv6 address 2002:A8c:C01::/128
tunnel source s1/0
tunnel mode ipv6ip 6to4
ipv6 route 2002::/16 tunnel0
ipv6 route 2001:A02:202::/64 2002 A8C:C02::
```

Troubleshooting 6to4 Tunnel

```
show ipv6 interface
show ipv6 interface brief
show ipv6 route
```

Configuring IPv6

```
(config)#ipv6 unicast-routing
(config)#no ipv6 unicast-routing
```

→ Enable IPv6 packet forwarding!
→ Disable IPv6 packet forwarding!

```
ipv6 cef
ipv6 flowset
```

→ Flow-label marking with 1280-byte or larger will be enabled.
Allows tracking of destinations.

```
ipv6 address [../length]
ipv6 address [prefix/length eui64]
(config-if)#ipv6 address autoconfig
(config-if)#ipv6 address dhcp
```

→ Use Stateless Autoconfiguration

```
ipv6 unnumbered [if]
ipv6 enable
ipv6 address [address] link-local
ipv6 address [address/length] anycast
```

Apply IPv6 ACL to an interface

```
ipv6 traffic-filter
```

Configuring the NS interval

```
ipv6 nd ns-interval [ms]
```

Configuring the "other stateful configuration"

- On = Use statefull autoconfiguration to obtain the other (nonaddress) information.

```
ipv6 nd other-config-flag
```

Configuring the "managed address configuration flag"

```
ipv6 nd managed-config-flag
```

Troubleshooting IPv6

```
#show ipv6 route
#show ipv6 protocols
show ipv6 neighbors
show ipv6 routers
```

→ Verify interfaces assigned to OSPFv3

```
#show ipv6 interface [IF]
#show ipv6 interface brief
```

```
#show ipv6 ospf
#show ipv6 ospf database
#show ipv6 ospf interface
#show ipv6 ospf interface brief
```

→ Verify interfaces assigned to OSPFv3
cost, state, area, number of neighbors

```
#show ipv6 ospf statistics
```

```
#debug ipv6 nd
```

ENHANCED SWITCHED TECHNOLOGIES

Spanning Tree Protocol (STP, IEEE 802.1D)

- Developed by **Radia Perlman**
- Also, called 802.1D-1998
- Link management protocol
- Loop avoidance on the **Data Link Layer**
- Created by Digital Equipment Corporation (**DEC**)
- IEEE created than **802.1D**
- Cisco moved than to **802.1W**
- **STP** uses the **Spanning Tree Algorithm (STA)**
- The use of **redundant connections** within a LAN-Design assures, that the LAN is also functioning if one or more switches fails.
- **STP** is activated by **default** on Cisco devices.
- If a Switch fails, **STP** needs usually **50 sec.** to recover the paths. Rapid Spanning Tree Protocol (RSTP) improves the time to recover.
- It's common practice to **leave STP enabled**, even if you do not have any cabling loops.
- Default **HELLO** time **2 seconds**.
- STP multicast MC address **01-80-c2-00-00-00**.
- The default value of the Forward Delay Timer is **15 seconds** (Listening → Learning).
- Default Max Age Time is **20 seconds**.
- The **location of the root bridge** should be determined as part of the design process.
- Cisco added two STP features that help preventing wrong switches to become Root: **Root Guard** and **BPDU Guard**.
- The STP topology's integrity depends on a **continuous and regular flow of BPDUs** from the root.
- Cisco has added two STP features that help detect or prevent the unexpected loss of BPDUs. **Loop Guard** and **UDLD**.
- A topology change typically takes **30 second**.

If no **STP** is used, the following problems may occur:

- Broadcast Storm
- Multiple frame copies
- Instable MAC-Tables
- MAC table trashing

STP is blocking dedicated interfaces to avoid the above-mentioned problems.

	Standard	Resources Needed	Convergence	
CST	802.1D	Low	Slow	All VLANs
PVST+	Cisco	High	Slow	Per VLAN
RSTP	802.1w	Medium	Fast	All VLANs
PVRST+	Cisco	Very high	Fast	Per VLAN
MSTP	802.1s Cisco	Medium or high	Fast	VLAN list

Figure 56: STP Overview

STP-Modes

- **IEEE 802.1d Common Spanning Tree (CST)**
The original standard for bridging and STP.
All CST BPDUs are transmitted over trunk link using the native VLAN with untagged frames.
1 instance of STP, over the native VLAN. 802.1q based.
- **PVST Per-VLAN Spanning Tree**
Cisco's proprietary enhancement for STP.
Operates a separate instance of STP for each individual VLAN.
Requires the use of Cisco Inter-Switch Link (ISL) trunking encapsulation between switches.
1 instance of STP per VLAN. Cisco ISL based.
- **PVST+ Per-VLAN Spanning Tree Plus**
Cisco's proprietary enhancement for STP.
Provides separate 802.1d spanning tree instances for each VLAN
Uses 802.1q to tunnel information's.
Provides interoperability between CST and PVST. Operates over both 802.1q and ISL.
- **RSTP / IEEE 802.1w Rapid STP**
The bridge resources used with RSTP are higher than CST's but less than PVST+
Allows only one root bridge per network like CST.
- **Rapid PVST+ (802.1q)**
Cisco's version of RSTP
Requires the most CPU and memory of all.
Provides a separate instance of 802.1w per VLAN.
UplinkFast can be disabled
BackboneFast can be disabled


```
(config)#spanning-tree mode rapid-pvst
```
- **IEEE 802.1s Multiple Spanning Tree (MST)**
Maps multiple VLANs into the same spanning-tree instance to save processing on the switch.
It basically rides on top of another spanning-tree protocol.

There are two modes: **Forwarding** or **Blocking**

STP Timers

- The STP timers are:
hello-time
forward-time
age time
- The timers need to be modified only on the **root bridge**.

Spanning Tree Algorithm (STA)

- **STP** chooses a **Root-Bridge/-Switch (RB)**
A good design allows to predict the Root-Switch (Set Priority).
Root-Switches do not have a Root-Port (RP).
The switch with the lowest Bridge ID becomes **RB**.
- Each **Not-Root-Bridge/-Switch (NRB)** chooses a **Root-Port** upon Root-Cost.
4 Mbps = 250 Root Cost
10 Mbps = 100 Root Cost
16 Mbps = 62 Root Cost
45 Mbps = 39 Root Cost
100 Mbps = 19 Root Cost
155 Mbps = 14 Root Cost
622 Mbps = 6 Root Cost
1 Gbps = 4 Root Cost
10 Gbps = 2 Root Cost
Each Not-Root-Switch has exactly one Root-Port.
NRBs exchange BPDUs with all other bridges and update the STP topology database.

- One of the switch will become the **Designated-Switch** with a **Designated-Port** (DP)

Bridge-ID (BID)

- Used by **STP** to keep track of all switches in the network.
- Formed initial by the **MAC-Address + Priority** (Default 32768).
- **Priority value** range 0-65535
- **Total 8 Byte** Field
- **2 Bytes Priority**
4 bits Priority + 12 Bits Extended System ID (VLAN-ID, 0, 4096, 8192, 12288 up to 61440)
32'768 by default on Cisco switches.
- **6 Bytes Extended System-ID** (MAC-Address)
The switch with the **lowest MAC address** will be used if all priorities are equal
- The **Extended System ID** portion of the BID is used to identify the **VLAN ID**

Bridge Protocol Data Units (BPDU)

- After the Root Switch is appointed, only this will send **Hello BPDU's** every **2 sec.**
- Inside the BPDU is the **Bridge-ID**
- The **root cost** will be **zero (0)**

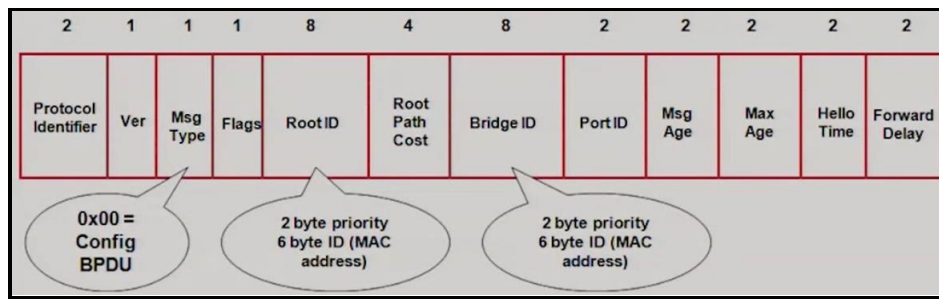


Figure 57: BPDU Frame Format

Port Cost

- Port cost determines the best path when multiple links are used between two switches.
- The cost of a link is determined by the bandwidth of a link.

Path Cost

- All unique paths are analyzed individually, and a path cost is calculated for each unique path by adding the individual port cost encountered on the way to the **RB**

Bridge Port Roles

- **Root Port**
Is the port with the lowest path cost to the **RB**. The RB has never a Root Port designated
- **Designated Port**
Lowest cost to a given network.
Is responsible to forward BPDUs.
Is always in **Forwarding** state.
- **Non-Designated Port**
Higher cost as the Designated Port
- **Forwarding Port**
Either a designated port or a root port
- **Blocked Port**
Listens to BPDUs but does not forward frames
- **Alternate Port**
- **Backup Port**

STP-Status:

Blocking / Forwarding / Listening / Learning / Disabled

802.1D State

Disabled
Blocking
Listening
Learning
Forwarding

802.1W State

Discarding
Discarding
Discarding
Learning
Forwarding

STP-Timer:

Hello every 2 sec.
Max Age Hello x 10
Forward-Delay 15 sec.

Convergence

- STP (802.1D) takes **50 seconds** to go from blocking to forwarding mode by default.

Link Costs

Port cost is the cost of a single link whereas **path cost** is the sum of the various port costs to the RB.

<u>Speed</u>	<u>Link Cost</u>
10 Mb/s	100
100 Mb/s	19
1000 Mb/s	4
10'000 Mb/s	2

Root Bridge Election

- **Port-priority** can range from **0 to 255**.
- **Default** port-priority is 128.

1. Lowest bridge ID
2. Lowest root path cost
3. Lowest sender bridge ID
4. Lowest sender port ID

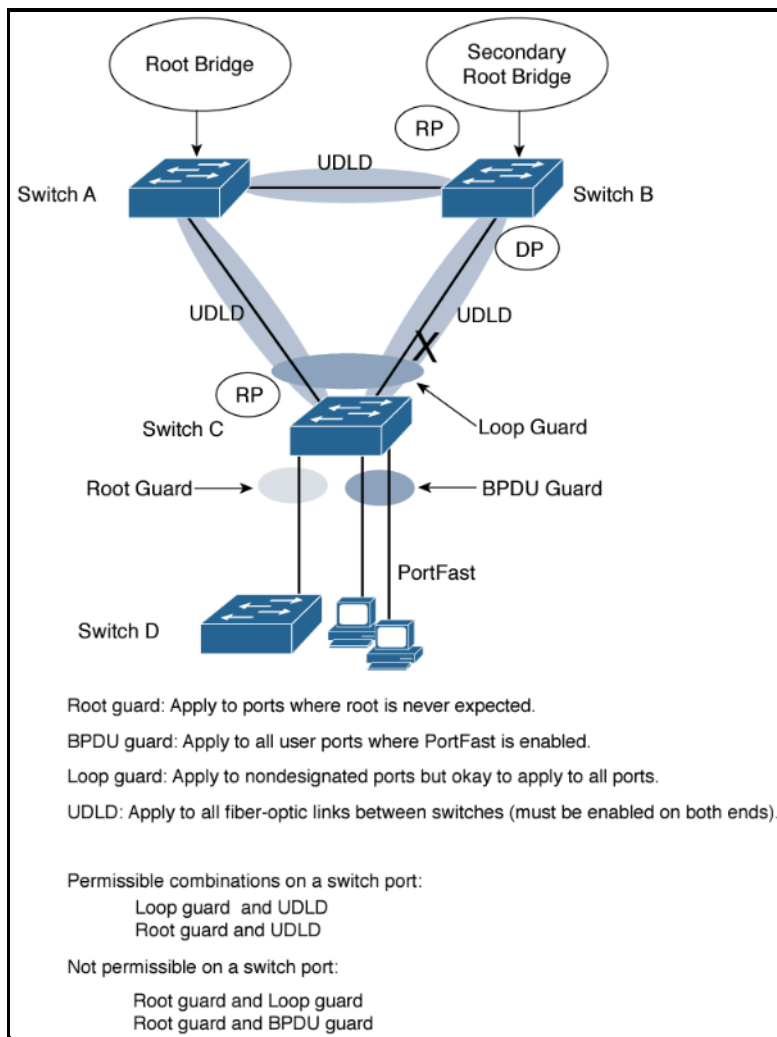


Figure 58: Guidelines for applying STP Protection Features

Root Bridge Placement

- If the root bridge election is left to its default state, several things can occur to result in a poor choice.
- For example the **slowest switch** could be elected as the root bridge.
- Determine the root bridge in the **distribution layer** or core layer, never in the access layer.

Configuring STP

- Configure one switch as a root bridge in a determined fashion.
- Configure another switch as a secondary root bridge, in case of a primary root bridge failure.
- Use one of the STP formats 802.1D or 802.1T.

```
(config)#spanning-tree vlan [x] root primary
(config)#spanning-tree vlan [x] root secondary
(config)#spanning-tree vlan [x] priority [0, 4096, ...]
```

Set Bridge Priority

```
(config-if)#spanning-tree vlan [VID] priority [x]
(config)#spanning-tree vlan [x], [100-200] priority 4096
```

Set Path Cost

- Range 1 to 200'000'000

```
spanning-tree cost [x]
(config-if)#spanning-tree [VID] cost [cost]
```

```
#set spantree root 1
#set spantree priority 8192 1
```

802.1T

```
(config)#spanning-tree extended system-id
```

Modify STP timers

```
(config)#spanning-tree [vlan VID] hello-time [sec]
(config)#spanning-tree [vlan VID] forward-time [sec] → Default 15 sec.
(config)#spanning-tree [vlan VID] max-age [sec] → Default 20 sec.
```

Troubleshooting STP

1. Find your **root bridge** by looking at bridge IDs
2. Determine your root ports by finding the lowest path cost to the bridge
3. Find your designated ports by looking at bridge IDs
4. Assure that the maximum STP dimension of 7 bridge hops is not exceeded
5. Check if also **HSRP**, **VRRP** or **GLBP** is configured, this can lead to **non-optimal traffic paths**.

```
show spanning-tree
    root bridge, root ports and designated and blocking/discarding ports
```

```
show spanning-tree [VID]
show spanning-tree detail
show spanning-tree summary
show cdp neighbors
```

```
show spanning-tree root
show spanning-tree mode pvst
show spanning-tree mode rapid-pvst
show spanning-tree mode mst
show spanning-tree vlan x
show spanning-tree vlan x root
```

```
spanning-tree vlan 2 priority [x 4096]
spanning-tree vlan 3 root primary
```

```
#show spanning-tree interface [type] [member | module | number]
```

```
#debug spanning-tree switch state
```

Troubleshooting STP Protection

```
#show spanning-tree inconsistentports
#show spanning-tree interface
#show spanning-tree summary
#show spanning-tree uddl
```

```
#uddl reset
```

Loop Guard

- By **default**, Loop Guard is disabled on all switch ports.
- The last-known BPDU is kept until the max age timer expires.
- See also Loop Guard STP feature.
- Loop Guard keeps track of the BPDU activity on nondesignated ports.
- When BPDUs go missing, Loop Guard moves the port into the **loop-inconsistence state**.

UDLD - Unidirectional Link Detection

- **Cisco proprietary**.
- You safely can **enable UDLD** on all switch ports.
- UDLD makes some intelligent assumptions when it is enabled on a link for the first time.

Normal Mode

Aggressive Mode

- UDLD disables the link if the neighbor does not reflect the message back within certain time.

Rapid STP (RSTP, 802.1w)

- **Advanced Spanning Tree Protocol.**
- Reduces the recovery time in case of failure to **max. 10 sec.**
- After a topology change RSTP, deletes immediately all MAC addresses that were learned dynamically in the same STP instance.
- Expands the STP port roles with **alternate** and **backup** roles

RSTP Port Behavior:

- Root Port
- Designated Port
- Blocking Port (neither root nor designated)

Five Possible States:

- Disabled
- Blocking
- Listening
- Learning
- Forwarding

PVRST+

```
(config)#spanning-tree mode rapid-pvst
#show spanning-tree
#show spanning-tree vlan [x]
```

MST - Multiple STP

MSTP+

- Multiple STP.

```
(config)#spanning-tree mode mst
(config)#spanning-tree mst configuration
(config-mst)#name [x]
(config-mst)#revision 1
(config-mst)#instance 1 vlan 11,21,31
(config-mst)#instance 2 vlan 12,22,32
(config)#spanning-tree mst 1 root primary
#show spanning-tree mst configuration
```

MANAGING CISCO DEVICES

Default order of IOS loading:

1. Flash
2. TFTP-Server
3. ROM

confreg 0x2142

Integrated Services Router (ISR)

- Cisco Integrated Services Router **Generation 2 (ISR G2)** delivers a new borderless workspace experience through **service virtualization, video-ready capabilities**.

Cisco 800 Series

Cisco 1900 Series

Cisco 2900 Series

Cisco 3900 Series

DHCP Snooping

- DHCP snooping is a **layer 2 security feature** that validates DHCP messages by acting like a firewall between untrusted and trusted servers.
- **Trusted interfaces** allow all type of DHCP messages and **untrusted interfaces** allow only requests.
- With DHCP snooping the switch builds a **DHCP snooping binding database**, where each entry includes the MAC and IP address.
- It checks if the **source MAC** and **client MAC** addresses are matching.

See also: **Dynamic ARP inspection (DAI)**

```
#ip dhcp snooping trust
```

RADIUS - Remote Authentication Dial-in User Service

Transport: Uses **UDP Port 1812**

- **Centralizes authentication** for remote connections.
- Can be implemented with **callback security**.
- Basically, a security system that works to guard the network against unauthorized access.
- RADIUS implements a **client/server architecture**, where the typical client is a router or switch and the typical server is a Windows or Unix device running RADIUS software.
- The RADIUS server also provides **AAA services** for multiple remote access servers.
- **AAA** = Authentication, Authorization and Accounting
- It encrypts only the **password** in the access-request packet, from the client to the server. The remainder of the packet is **unencrypted**.
- It **combines authorization** and **accounting** functions.
- The **network access server** is the client of the RADIUS authentication server.

Authentication process:

1. The user is prompted for a username and a password
2. The username and encrypted password are sent over the network to the RADIUS server
3. The RADIUS server replies with either:
Accept, Reject, Challenge or Change Password

Configuring RADIUS

```
(config)#aaa new-model → Activates authentication on all lines except the console
(config)#username [name] password [pwd] →

(config)#radius server SecureLogin →
(config-radius-server)#key [MyRadiusPassword]
(config)#aaa group server radius MyRadiusGroup
```

```
(config-sg-radius)#radius server SecureLogin
(config)#aaa authentication login default group myRadiusGroup local
```

Troubleshooting RADIUS

```
#show aaa servers
#show radius-server-group

#show ip route
#show ip interface brief
```

TACACS+ - Terminal Access Controller Access Control System

Transport: Uses **TCP Port 49**.

- **Cisco proprietary** security server, like RADIUS
- TACACS+ **separates authentication, authorization** and **accounting**, RADIUS not.
- Provides separate **AAA services**.
- **Encrypts** an entire packet.
- Offers **multiprotocol support**.
- Mainly used for **device administration**.
- Supports **15 privilege levels**.
- **TACACS** and **XTACACS** are older versions which are using **UDP port 49**.

Configuring TACACS+

```
(config)#aaa new-model → Activates authentication on all lines except the console
(config)#username [name] password [pwd]

(config)#radius server SecureLoginTACACS+
(config-radius-server)#address ipv4 10.10.10.254
(config-radius-server)#key [MyTACACS+Password]
(config)#aaa group server radius MyTACACS+Group
(config)#server name SecureLoginTACACS+
(config)#aaa authentication login default group myTACACS+Group local
```

Troubleshooting TACACS+

```
#show aaa servers
#show radius-server-group

#show ip route
#show ip interface brief
```

Diameter

Transport: Uses **TCP Port 3868**.

- An enhanced version of **RADIUS**.
- Popular if **s** is required, such as with **wireless devices**.
- It is **not backward compatible** to RADIUS:
- It also supports **IPSec** and **TLS** for encryption.

Switch Stacking

See also: Cisco StackWise technology

- The **master switch** manages the stack as single unit.
- You can join up to **9** separate switches in a **StackWise** unit.
- Each stack has a **single IP address**.
- There is **no designated backup master switch**, the new master is selected by election.

Pros

- You can add more ports by avoiding upgrading to a bigger switch.
- Stacks are managed as a single unit, which reduces the management effort.
- You can add or remove switches without disrupting the network.
- **STP** is no longer needed if you use EtherChannel
- If you add a new switch, the master switch **automatically configures the unit**.

Cons

- You must use special stack interconnection cables.

Cisco FlexStack/FlexStack-Plus

- All switches in a FlexStack or FlexStack-Plus stack are acting as a single switching unit.
- Especially used with Cisco Catalyst 2960-Series
- FlexStack-Plus doubles the speed of the stack from 20 Gbps to 40 Gbps bandwidth and allows for 8 members to join the stack, instead of 4.
- FlexStack-Plus stack convergence is now 100 ms instead of 1-2 sec
- FlexStack-Plus link failure detection is now in hardware

FHRP - First-Hop Redundancy Protocols

- **FHRP** work by giving you a way to configure more than one physical router to appear as if they were only a single logical one.
- **First hop** is a reference to the default router being the first router, or first router hop, through which a packet must pass
- Several routers can be installed and are used as a single **Default-Gateway** (Virtual Router).
- This avoids **Single-Point-Of-Failures**.

FHRP defines a group of protocols, such as:

- **Hot Standby Routing Protocol (HSRP)** active/standby
Virtual IP-Address + Virtual MAC-Address
- **Virtual Router Redundancy Protocol (VRRP)** active/standby
- **Gateway Load Balancing Protocol (GLBP)** active/active
Allows Load balancing

Active Virtual Gateway (AVG)

HSRP - Hot Standby Router Protocol

- Is a **Cisco proprietary protocol**.
- Technique for redundant routers.
- Usually **dynamic routing** assures availability of the paths, but if the first router fails, **dynamic routing** cannot cover this situation, since a host knows only one default gateway(router).
- HSRP builds with two or more routers a logical router.
- The logical router gets a **virtual IP-Address** and a **virtual MAC-Address** (Prefix: **00-00-0c-07-ac...**) and is bound to a one physical router, which will be the **primary-router**.
- If the primary-router fails, another physical-router becomes the primary-router (within ~10sec).
- A **virtual router** in an HSRP group has a **virtual IP** address and a **virtual MAC address**.
- Today the following values are used: **Hello Timer 200 msec** and **Hold Timer 700 msec**
- The router with the **highest priority** will win the election and become the **active router**
- HSRP does not really perform **true load balancing**, but per **VLAN** a sort of.
- Devices participate in a **HSRP group**
Up to **256 groups, 0 - 255** on Ethernet
- HSRP supports up to **255 groups per interface**, enabling an administrative form a **load balancing**.
- **HSRPv2** support 0 - 4095 groups
- **Default priority** of an HSRP interface = **100**.
- **Active forwarders** = **1**.
- **Preemption** is **OFF** by default.
- Two devices share the same virtual IP and MAC address
00-00-0C-07-AC-XX
XX = Represents the group number
- Uses the multicast address **224.0.0.2** for communication
Port 1985
Packets are exchanged every 3 seconds
Dead timer is 10 seconds
-

Hello Timer

- Each router sends Hello messages by default every **3 seconds**.

Hold Timer

- Specifies the (dead) interval, the standby router uses to determine whether the active router is offline or out of communication (Default: **10 seconds**)
- The hold timer should always be **~3 times** the Hold Time

Active Timer

- Monitors the state of the active router.

Standby Timer

- Monitors the state of the standby router.

Group Roles

- Virtual Router
- Active Router
- Standby Router
- Other Routers

HSRP States

- Learn
- Listen
- Speak

HSRP States

- Initial - Not running
- Learn
- Speak - Sends "hellos"
- Standby
- Active

HSRP Virtual IP

- The virtual router IP address must be an unused IP in the LAN.

HSRP Virtual MAC Address

- e.g. VMAC 0000.0c07.ac0a

0000.0c (Vendor Code)
 07.ac (Well-known HSRP Code)
 0a (HSRP Group number 10 in hex)

Configuring HSRP

Router1

```
(config-if)#standby 1 ip 10.1.1.10
(config-if)#standby 1 priority 150      → Sets the router to the active one
(config-if)#standby 1 preempt      → Sets the router to the active one

(config-if)#standby 1 track int_type int_no decrement_value      → Set Interface Trackin
```

Router2

```
(config-if)#standby 1 ip 10.1.1.10
```

Troubleshooting HSRP

```
#show standby      → Shows the virtual MAC
#show standby brief      → Which int is participating in a HSRP Group
#show standby Fa0/0      → Shows the MAC Address
```

```
debug standby terse
```

VRRP - Virtual Router Redundancy Protocol

RFC 2338, 5798

Transport: IP protocol number **112**.

- The **Virtual Router Redundancy Protocol (VRRP)** is a computer networking protocol that provides for automatic assignment of available @Internet Protocol (IP) routers to participating hosts.

- This increases the availability and reliability of routing paths via automatic default gateway selections on an IP sub network.
- The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group.
- The default gateway of a participating host is assigned to the virtual router instead of a physical router.
- If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it.
- VRRP provides information on the state of a router, not the routes processed and exchanged by that router.
- Each VRRP instance is limited, in scope, to a single subnet.
- It does not advertise IP routes beyond that subnet or affect the routing table in any way.
- VRRP can be used in **Ethernet**, **MPLS** and **token ring** networks with **@Internet Protocol Version 4 (IPv4)**, as well as **IPv6**.
- Cisco claims that a similar protocol with essentially the same facility is patented and licensed.

Source: Wikipedia

- VRRP is the **open standard-based** alternative to HSRP.
- VRRP has only **minor differences** to HSRP.
- VRRP allows a group of routers to form a **single virtual router**.
- VRRP provides **one redundant gateway address** from a group of routers.
- The **master virtual router** may have the **same IP address as the virtual router group**.
- VRRP is supported on **Ethernet**, **Fast Ethernet**, **Gigabit Ethernet**, **MPLS**, **VPNs** and **VLANs**
- **VRRP groups** numbers range from **0 to 255**.
- **Router priorities** range from **1 to 254** default is **100**.
- The **virtual router MAC address** is of the form **0000.5e00.01xx**, where **xx** is a two-digit hex VRRP group number.
- VRRP **advertisements** are sent at **1 second** intervals to the multicast address **224.0.0.18**.
- **Preemption** is **ON** by default.

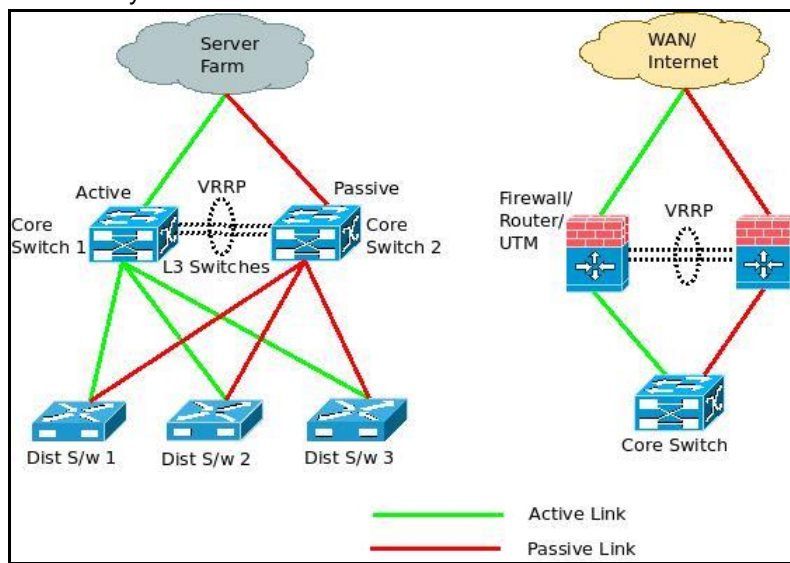


Figure 59: VRRP

VRRP Virtual Router Master

- The name for the router in a **VRRP virtual router group** that is actively forwarding traffic.
- A **VRRP group** has **one master router** and one or more **backup routers**.
- The **master router** uses **VRRP messages** to inform group members of its status.
- The **master router** is the one with the **highest router priority** in the VRRP group.

VRRID - Virtual Router Identifier

- e.g. VMAC 0000.5e00.0114

```
0000.5e (Vendor Code/IANA)
00.01 (Well-known VRRP Code)
0a (VRRP Group number 10 in hex)
```

VRRP Virtual IP

- The **virtual router IP** address can be an unused IP in the LAN or an IP associated with a router's LAN interface.

Configuring VRRP

```
(config-if)#vrrp [group] priority [level]
(config-if)#vrrp [group] timers advertise [msec] interval
(config-if)#vrrp [group] timers learn
(config-if)#no vrrp [group] preempt
(config-if)#vrrp [group] preempt [sec]
(config-if)#vrrp [group] authentication [string]
(config-if)#vrrp [group] ip [IP] [secondary]
(config-if)#vrrp [group] track [x] [decrement priority]
```

Troubleshooting VRRP

```
#show vrrp
#show vrrp brief
#show vrrp interface vlan <nr>
#show track → Object tracking
```

GLBP - Gateway Load Balancing Protocol

- **Cisco proprietary protocol.**
- Only the active routers in **HSRP** and **VRRP** groups forward traffic for the **virtual MAC**.
- The **active virtual gateway** will reply to client ARP requests with **one of four** possible virtual MAC addresses
- **Active/active** approach on a **per-subnet** basis.
- GLBP can perform **per-host** load balancing
- **Hello Messages** every **3 seconds** to **224.0.0.102**
- GLBP provides **upstream load-sharing** by utilizing the redundant uplinks simultaneously.
- **GLBP group** can have up to **four group members**.
- GLBP uses the **round-robin** algorithm.
- Supports **clear text** and **MD5** password authentication between GLBP members.
- GLBP allows **multiple routers** to simultaneously forward traffic.

AVG - Active Virtual Gateway

AVF - Active Virtual Forwarder

Virtual Router MAC Addresses

- e.g. VMAC 0007.b400.2b02

```
0007.b400 (Well-known GLBP Code)
2b (GLBP Group no.)
02 (AVF ID)
```

Configuring GLBP

```
(config-if)#glbp 1 ip x.x.x.x
(config-if)#glbp 1 name [x]
(config-if)#GLBP 1 priority 110
```

Toubleshooting GLBP

```
show standby
show standby brief
show glbp
show glbp brief
```


IP SERVICES

- **Proxy ARP** enables hosts, which have no knowledge of routing options, to obtain the MAC address of a gateway router that can forward packets for them.

Syslog / Logging

- **Traffic telemetry** method.
- System messages are logged in buffers in RAM
- Cisco's default logging to the console is **7** (Debugging)
- Logging buffer (on by default)
- Console line (on by default)
- Terminal lines (using the terminal monitor command)
- Syslog server.

Logging Categories (*dinwecae*)

- Below the log message categories with the most severe at the top:

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Mnemonic	Severity	Description
%SEC-6-IPACCESSLOGDP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGNP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGP	6	A packet matching the log criteria for the given access list has been detected (TCP or UDP)
%SEC-6-IPACCESSLOGRL	6	Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available.
%SEC-6-IPACCESSLOGRP	6	A packet matching the log criteria for the given access list has been detected.
%SEC-6-IPACCESSLOGS	6	A packet matching the log criteria for the given access list was detected.
%SEC-4-TOOMANY	4	The system was not able to process the packet because there was not enough room for all of the desired IP header options. The packet has been discarded.
%IPV6-6-ACCESSLOGP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGDP	6	A packet matching the log criteria for the given access list was detected.
%IPV6-6-ACCESSLOGNP	6	A packet matching the log criteria for the given access list was detected.

Timestamp Symbols

- Preceding dot (.) indicates that the time is authoritative.
- * The time is NOT authoritative.

Configure Logging

```
(config)#logging [ip | hostname]
(config)#logging console
(config)#logging buffered
(config)#logging synchronous
```

→ Prevents syslog messages from interrupting commands

```
(config)#logging trap 6
(config)#logging trap warnings
```

```
(config)#service timestamps log datetime [msec]
```

(config)#service sequence-numbers → Will display messages with sequence numbers

Troubleshooting Logging

#show logging

Configure Logging on ATA Flash disk

logging buffered → Enables system message logging
logging persistent url disk1:/syslog size 134217728 filesize 16384

Debug Command

- Should be carefully used because of Overhead.

show debugging → Which type of debugging is enabled

debug all →

debug [protocol] →

#debug ip bgp →

#debug ip bgp x.x.x.x →

#debug ip icmp →

#debug modem →

#debug ppp negotiation →

#debug ip tcp →

#debug ip tcp packet →

#debug ip tcp transactions →

Cisco Network Services (CNS)

- CNS agents is a **collection of services** that can provide **remote event-driven configuring** of Cisco IOS networking devices and **remote execution** of some command-line interface (CLI).
- CNS has been designed to provide **“plug-and-play”** network services using a central directory service and distribution agents.

Configure CNS

(config)#cns config

Simple Network Management Protocol (SNMP)

RFC 1065

Transport: Uses **UDP port 161**.

- SNMP was created in **1988**
- SNMP is an **Application Layer** protocol
- **Traffic telemetry** method.
- SNMP provides message format for Network Management Stations (**NMSs**) like **Cisco Prime** or **HP Openview**
- The information will then be written in the NMS **Management Information Base (MIB)**
- Monitoring of Network components
- Remote control and configuration of Network components
- Message alert

There are **three versions** of SNMP:

SNMPv1 Supports plaintext authentication with community strings and uses only UDP

SNMPv2 Supports plaintext authentication with community strings with no encryption but provides

GET BULK to reduce the number of GETs. It offers a more detailed error message reporting method called INFORM. But it's not more secure than v1. It used UDP and can use TCP.

SNMPv3 Supports strong authentication with MD5 or SHA and encryption with DES or DES-256. It allows user-based access. It uses UDP and TCP

Needs:

Managementconsole
Agents

Configuring SNMP

1. Enable SNMP read-write access to the device
2. Configure SNMP contact information
3. Configure SNMP location
4. Configure ACL to restrict SNMP access to the NMS host

```
(config)#snmp-server community [x] rw
(config)#snmp-server location [x]
(config)#snmp-server contact [x]
(config)#ip access-list standard [Protect_NMS]
(config-std-acl)#permit host 192.168.10.254
```

```
(config)#snmp-server engineID local
(config)#snmp-server engineID remote
```

```
-----
snmp-server host [IP] traps version 2c [pwd]
snmp-server manager → Starts the SNMP manager process
```

Troubleshooting SNMP

```
#show snmp
#show snmp group
#show snmp pending
#show snmp sessions
#show snmp engineID
#show management event
```

Configuring SNMPv3

1. Configure the server group
2. Create a user for each group

```
(config)#snmp-server group [lmsgrp] v3 auth
(config)#snmp-server group [nmsggrp] v3 auth write vlddefault
```

```
(config)#snmp-server user lmsuser lmsgrp v3 auth md5 lmsuser123
(config)#snmp-server user nmsuser nmsggrp v3 auth md5 nmsuser123
```

```
-----
priv → Offers authentication and encryption
authnopriv → Offers authentication unencrypted
```

```
(config)#snmp-server group [lmsgrp] v3 [auth|noauth|priv]
```

Troubleshooting SNMPv3

```
#show snmp groups
#show snmp user → Shows: Authentication Protocol and Privacy Protocol
#show snmp user [user_name]
```

SMIv1/SMIv2 Structure of Management Information Version X

- In computing, the **Structure of Management Information (SMI)**, an adapted subset of ASN.1, operates in Simple Network Management Protocol (SNMP) to define sets ("modules") of related managed objects in a Management Information Base (MIB).
- SMI subdivides into three parts:
 - **Module definitions**
Module definitions are used when describing information modules. An ASN .1 macro,

MODULE-IDENTITY, is used to concisely convey the semantics of an information module.

- **Object definitions**
Object definitions describe managed objects. An ASN.1 macro, OBJECT-TYPE, is used to concisely convey the syntax and semantics of a managed object.
- **Notification definitions**
Notification definitions (aka "traps") are used when describing unsolicited transmissions of management information. An ASN.1 macro, NOTIFICATION-TYPE, concisely conveys the syntax and semantics of a notification

Source: Wikipedia

Management Information Base (MIB)

- The community string will authenticate your access to the MIB database.
- You must specify the version, community string, IP address and the OID number
- It's a good idea to monitor the **CPU** every **5 minute**

NetFlow

Transport: Data are sent using **UDP** port **9996** (Default).

- **Traffic telemetry** method.
- NetFlow is completely **transparent** to the users in the network.
- NetFlow enables near real-time **visualization** and **analysis** of recorded and aggregated **flow data**.
- You need a router enabled with NetFlow and a **NetFlow collector**.
- Data can be viewed with **CLI** or **NetFlow**.
- See also **NetFlow Data Export (NDE)**.
- The **NetFlow Management Information Base (MIB)** feature allows system information stored in the flow cache, such as IP flow information, to be accessed in real time.

NetFlow application, collects IP traffic information's such as:

- Network traffic patterns
 - Protocols
 - TCP/IP flows
- A **flow** is a unidirectional stream of packets between a source and destination host or system. Consisting of Source IP, Destination IP and Ingress Interface.
- Source IP address
 - Destination IP address
 - Source port
 - Destination port
 - Ingress physical interface index (defined by SNMP)
 - Egress physical interface index (defined by SNMP)
 - Packet count for this flow
 - Byte count for this flow
 - Start of flow timestamp (FIRST_SWITCHED)
 - End of flow timestamp (LAST_SWITCHED)
 - IP protocol number
 - TCP flags from the flow (TCP only)

ISPs use NetFlow to:

- Efficiently measure who is using network services and for what purpose.
- Accounting and charging back according to the utilization.
- For network planning.
- For better structuring the applications.
- Showing the major users of the network.
- Monitoring the websites and what was downloaded.
- Who's generating the most traffic and using excessive bandwidth.

In General:

- Application and network usage
- Network productivity and utilization of network resources
- The impact of changes to the network
- Network anomaly and security vulnerabilities
- Long term compliance issues

NetFlow Inspection:

Uses:

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- Layer 3 Protocol
- ToS Byte (COS, DSCP)
- Input Interface

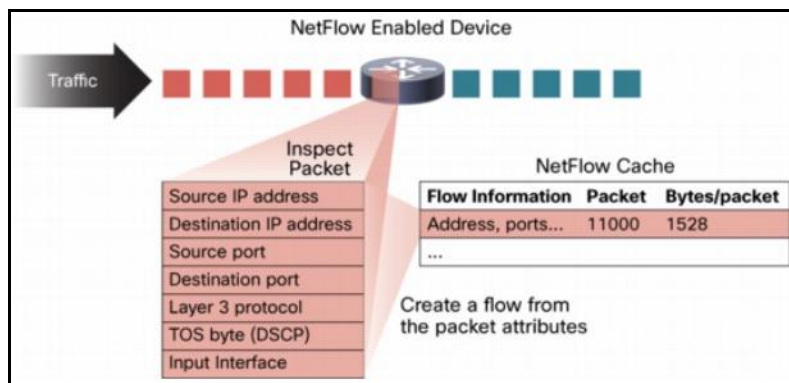


Figure 60: NetFlow Inspection

Random Sampled NetFlow

- Random Sampled NetFlow provides NetFlow data for a **subset** of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter).
- Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets).
- Statistical traffic sampling substantially **reduces consumption of router resources** (especially CPU resources) while providing valuable NetFlow data.

Configuring NetFlow

```
(config-if)#ip flow ingress          → Incoming packets
(config-if)#ip flow egress          → Outgoing packets

(config)#ip flow-export destination [IP] [Port] →
(config)#ip flow-export version 9      → Define the format.
                                         Most current version = 9.
                                         Supports Multicast and BGP next-hop

(config)#ip flow-export source loopback 0 →
```

Configure multiple NetFlow export destinations.

```
(config)#ip flow-aggregation cache destination-prefix
(config)#export destination [IP1]
(config)#export destination [IP2]
...
```

Enable NetFlow accounting for IP routing.

```
ip route-cache
ip route-cache flow
```

Troubleshooting NetFlow

(config)# show ip flow interface	→
(config)#show ip flow export	→
(config)#show ip cash flow	→ Visualize NetFlow data
#show flow exporter [x]	→ Show the status of the exporter.

Per-Destination Load Balancing

- Per-destination load balancing allows the router to distribute packets based on the destination address, and uses **multiple paths** to achieve load sharing.
- Packets for a given source-destination host pair are guaranteed to take the same path, even if multiple paths are available. For example, given two paths to the same network, all packets for destination1 on that network go over the first path, all packets for destination2 on that network go over the second path, and so on.
- Per-destination load balancing is enabled by **default** when you start the router, and is the **preferred load balancing** for most situations

Per-Packet Load Balancing

- The Per-Packet Load Balancing feature allows data traffic to be evenly distributed in an IP network over **multiple equal-cost connections**.
- Per-packet load balancing uses **round-robin** techniques to select the output path without basing the choice on the packet content.

TROUBLESHOOTING IP, IPv6

Cisco's steps in troubleshooting *IPv4* and *IPv6* Problems:

1. Check the cables to find out if there's a faulty cable or interface in the mix and verify the interface's statistics.
2. Make sure that devices are determining the correct path from the source to the destination. Manipulate the routing information if needed.
3. Verify that the default gateway is correct.
4. Verify the name resolution settings are correct.
5. Verify that there are no access control lists (ACLs) blocking traffic.

Four steps for checking PC configuration:

1. Test that the local IP stack is working by pinging the loopback address.
2. Test that the local IP stack is talking to the Data Link layer (LAN driver) by pinging the local IP address.
3. Test that the host is working on the LAN by pinging the default gateway.
4. Test that the host can get to remote networks by pinging remote Server.

```
show ipv6 int brief
show ipv6 neighbors
show ipv6 route
show ipv6 access-lists
```

Disable Temporary IPv6 Addresses (Windows):

See: Communication General.docx

IP SLA - IP Service-Level Agreement

- Monitors **network health** and **reachability**.
- Causes the router to **create packets locally**.
- Uses the concept of **operation**. Each operation defines a type of packet that the router will generate, the destination and source address, and other characteristics of the packet.
- Earlier versions of IP SLA are **Response Time Reporter (RTR)** which can be set with the command **rtr**.
- Instead of **ICMP** also **HTTP GET** can be used.
- Also, RTP, TCP connection, UDP, DNS, DHCP, and FTP can be used as **operation**.
- Stores the statistics in the **CISCO-RTTMON-MIB**.
- It supports **problem isolation** and **network planning**.
- IP SLA **Threshold violations** are logged as **level 6-Informational** within the logging process, but are **sent as level 7-info traps** from the CISCO-SYSLOG-MIB.

Example of an **operation**:

- Use ICMP
- Measure the end-to-end RTT
- Send the packets every 5 minutes

Operation Types:

- ICMP (echo, jitter)
- RTP (VoIP)
- TCP connection (establishes TCP connections)
- UDP (echo, jitter)
UDP Jitter for VoIP requires Cisco endpoints
- DNS
- DHCP
- HTTP
- FTP

Network Performance Monitoring of:

- One-Way Delay
- Jitter

- Packet Loss
- Connectivity
- Packet Ordering
- Packet Corruption

```
ip sla responder [Options see below]
http
```

→ Measures round-trip time to retrieve a web page.

```
tcp-connect
```

→ Measures the time taken to connect to a target device with TCP.

Troubleshooting with IP SLA:

- Edge-to-edge network availability monitoring.
For example, packet loss statistics.
- Network performance monitoring and network performance visibility.
For example, network latency and response time.
- Troubleshooting basic network operation.
For example, end-to-end network connectivity

Cisco IOS IP SLAs Responder

- The Cisco IOS SLA Responder is only needed if the operation is not a normal function of the router. For instance, if the router answers to ICMP and this will be used as operation, no responder is needed.
- The Cisco IOS IP SLAs Responder is a component embedded in the destination Cisco routing device that allows the system to anticipate and respond to Cisco IOS IP SLAs request packets.
- The Cisco IOS IP SLAs Responder provides an enormous advantage with accurate measurements without the need for dedicated probes and additional statistics not available via standard ICMP-based measurements.
- The patented Cisco IOS IP SLAs Control Protocol is used by the Cisco IOS IP SLAs Responder providing a mechanism through which the responder can be notified on which port it should listen and respond.
- Only a Cisco IOS device can be a source for a destination IP SLAs Responder.

Tracking Object

- A **cross-reference** between the static route, PBR and IP SLA.

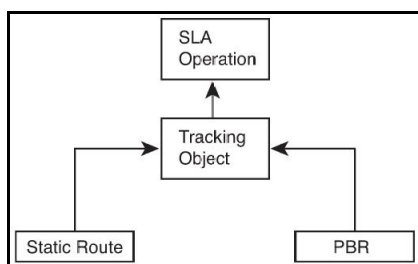


Figure 61: Relationship for Path Control using IP SLA

Configuring IP SLA ICMP Echo

```
(config)#ip sla 1
(config-ip-sla)#icmp-echo 172.16.20.254 → Operation type
(config-ip-sla-echo)#frequency [sec]
```

```
(config)#ip sla schedule 1 life forever start-time now
```

Configure a Tracking Object (Static Route)

```
(config)#track 2 ip sla 11 state
(config-track)#delay up 90 down 90
(config)#ip route 10.1.234.0 255.255.255.0 s0/0 track 2
```

Verify next-hop interface

```
set ip next-hop verify-availability 10.1.1.4.4 1 track 2
```

Threshold Setting

threshold [msec]

Troubleshooting IP SLA ICMP Echo

#show ip sla configuration

#show ip sla statistics

→ Displays measurements

#udp-jitter

→ Verifying one-way packet loss

#show track

→ Verifies the track/probe mapping

UDP

- Is considered **connectionless** and **unreliable**.
- The primary protocol to carry **voice** and **video**.
- Does not care of **sequencing**, this must be handled by the **application**.
- A UDP header is **8 bytes** (64 bits) long.

UDP Dominance

- Since TCP lowers its transmission rates while UDP continues to utilize the freed bandwidth, this effectively leads to a situation called **UDP dominance** or **TCP starvation**.
- UDP dominance can happen during **times of congestion**.
- When a link is fully utilized, **TCP** has automatic congestion avoidance and error discovery methods that allow it to know when to **slow down the sending rate**.
- On the contrary, **UDP** has no such mechanism. It keeps blasting the link with data, with absolutely no regard to how this may affect other traffic flows.
-

Jitter

- **Delay variation**.
- Is the undesired deviation from true periodicity of an assumed periodic signal in electronics and telecommunications, often in relation to a reference clock source.
- Jitter may be caused by electromagnetic interference (EMI) and crosstalk with carriers of other signals.
- The deviation from true periodicity of inter-packet gaps, it is measured for flows with three and more packets. In detail, it measures delay between **first** and **second packet** and then between **second** and **third packet**. The difference of these two values is jitter.
- IP SLA results are stored in the **CISCO-RTTMON-MIB**.
- The difference in the end-to-end delay between packets. For example, if one packet requires 100 ms to traverse the network from the source endpoint to the destination endpoint and the following packet requires 125 ms to make the same trip, then the delay variation is 25 ms.

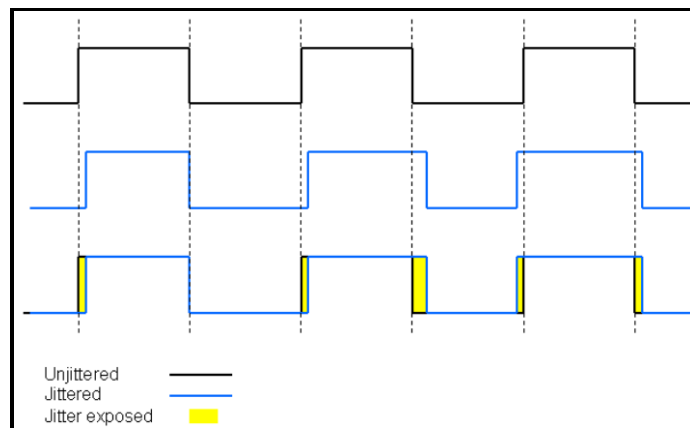


Figure 62: Jitter

Impact

- Jitter impacts mainly real time applications.

- Jitter can cause a display monitor to flicker, affect the performance of processors in personal computers, introduce clicks or other undesired effects in audio signals, and loss of transmitted data between network devices. The amount of tolerable jitter depends on the affected application.

Low Latency Queuing (LLC)

???

Helpdesk Templates

Help Desk Ticket	
Client Identifier:	
Issue:	
Detailed information about the issue	
Test:	
Test:	
Resolution:	

Help Desk Ticket	
Client Identifier: PC1	
Issue: Unable to access the dualstackserver.pka web page.	
Detailed information about the issue	
Test: Does the computer have an IP address using ipconfig ?	Yes
Test: Can the computer contact its gateway using ping ?	Yes
Test: Can the computer contact the server using tracert ?	Yes
Test: Can the computer contact the server using nslookup ?	No
Resolution: Escalate to Level 2 support.	

Help Desk Ticket	
Client Identifier: PC2	
Issue: Unable to access the FTP service of 2001:DB8:CAFE:1:10.	
Detail information about the Issue	
Test: Does the computer have an IPv6 address using ipv6config ?	Yes
Test: Can the computer contact its gateway using ping ?	Yes
Test: Can the computer contact the server using tracert ?	No
Resolution: Escalate to Level 2 support.	

Help Desk Ticket	
Client Identifier: PC3	
Issue: Unable to communicate with PC2.	
Detail information about the Issue	
Test: Does the computer have an IP address using ipconfig ?	Yes
Test: Does computer have an IPv6 address using ipv6config ?	Yes
Test: Can the computer contact its IPv4 gateway using ping ?	No
Test: Can the computer contact its IPv6 gateway using ping ?	Yes
Test: Can the computer contact the IPv4 client using tracert ?	No
Test: Can the computer contact the IPv6 client using tracert ?	Yes
Resolution: Escalate to Level 2 support.	

TROUBLESHOOTING VLANs

Troubleshooting VLAN:

1. Verify the VLAN database on all your switches
2. Verify your content addressable memory (CAM) table
3. Verify that your port VLAN assignments are configured correctly

Troubleshooting Trunks:

1. Verify that the interface configuration is set to the correct trunk parameters
2. Verify that the ports are configured correctly
3. <verify the native VLAN on each switch

```
show interfaces trunk
show vlan
show interfaces interface trunk
show interfaces interface switchport
show dtp interface [interface]
switchport mode
switchport mode dynamic
switchport trunk native vlan vlan
```

IGRP

- Predecessor of EIGRP.
- Sends updates every **90 seconds**.
- Don't support VLSM and discontinuous network.
- Periodic full routing updates.
- Not 100% loop free.

Troubleshooting IGRP

```
show ip interfaces
```

EIGRP

Enhanced Interior Gateway Routing Protocol (EIGRP)

Transport: Protocol number **88** (does not use UDP or TCP)

Authentication: EIGRP supports only **MD5 authentication**.

- EIGRP was in the beginning a proprietary **CISCO protocol**, it's **now released as RFC**.
- EIGRP is **vendor specific**.
- EIGRP is a **classless, distance-vector protocol** and is using the **concept of autonomous system** to describe the set of contiguous routers.
- Useful for **large, complex networks**.
- It supports **VLSM**.
- Automatically **summarizes** networks.
- EIGRP is **not based on areas** like OSPF.
- EIGRP **doesn't use Link-States**, it's using a **distance-vector logic** to calculate the best route.
- EIGRP is checking the state of the neighbors with **EIGRP-Hellos** which is sent by the protocol **Reliable Transport Protocol (RTP)** by default every **5 seconds**.
- Uses **multicast** instead of broadcast.
- To detect neighbors, EIGRP is using the **multicast address 224.0.0.10**.
- If no answer is received by the multicast, EIGRP will send **16 unicast messages** before declaring the route as dead.
- The prediction of the route with EIGRP is **complex** in comparison with OSPF.
- Default hop count **100**.
- Best path selection via **Diffusing Update Algorithm (DUAL)**.
- EIGRP is **load-balancing** by default if the route costs are equal on up to **32 links** (default 4 links).
- The **maximum hop count** is used to limit the AS.
- By default, a router sends EIGRP messages out an interface but only up to **50 percent** of the bandwidth defined on the interface with the **bandwidth** command.

- **Less network design constraints** than OSPF.
- EIGRP by default will use **up to 50% of the bandwidth** for EIGRP packets.
- **Default hold timers and hello timers** on interfaces/subinterfaces with a BW of T1 or lower and encapsulation type of Frame Relay is: Hold timer = 180 seconds and hello timer = 60 seconds.
- **Default BW** on serial interfaces and subinterface is 1544 Kbps.
- It provides **faster convergence** than other routing protocols.
- IT provides **seamless connectivity** across all **data-link layer protocols and topologies**.
- If the **network** command includes a **wildcard mask**, the router performs access control list (**ACL**) logic.
- Default seed metric **INFINITY** = 0.

Route-Poisoning is the function which advertises a route-outage.

- It advertises a metric that is higher than the maximum.

Split Horizon

- **Prevents** a route learned on one interface from being advertised back out of that interface.
- Is enabled by **default**.
- Assures that not all possible routes are advertised. This avoids routing loops.
Used in: RIP, EIGRP, IGRP and VPLS

Poison Reverse

- Causes a route received on one interface to be advertised **back out of that same interface** with a metric considered to be infinite.

The three major steps

1. **Establish** EIGRP neighbor relationship with other routers that share a common subnet.
Neighbor Discovery.
Before EIGRP routers can exchange routes, they must become neighbors.
Hello or ACK received
AS number match
Identical metrics (K values)
2. **Exchange** EIGRP topology data with those neighbors.
Topology Exchange.
3. **Calculate** the currently best IP route for each subnet, based on the known EIGRP topology data, and add those best routes to the IP routing table.
Choosing routes.

The **Hold timer** defines the time a router is willing to wait for a Hello before declaring him dead.

The **Neighbor table** contains information's of specific routers. It replaces the IPv4 ARP table:

- IP Address of neighbor
- Hold time
- Smooth round-trip timer (SRTT)
- Queue information

Topology table

- Contains **Successor** and **Feasible Successor (FS)** routes.
- All routes in the AS are stored in the topology table.

#show ip eigrp topology

P = Passive, EIGRP has found all usable paths

A = Active, EIGRP is still querying the path to a network.

Displays all FS, metrics and states.

Route table

1. Stores the routes that are currently in use.

Feasible successor (FS)

- A **FS** is a **backup route** and is stored in the **topology table**.

- Advertised distance (AD) or reported distance (RD) is the metric advertised by the next-hop router. You would consider this value to verify **feasible successors**.
- Immediately usable, **loop-free** route
- If a nonsuccessor route's RD is less than the **FD**, the route is a feasible successor route.

Feasibility Condition (FC)

- A neighbor meets the feasibility condition (FC) if the reported distance by the neighbor is the same as, or less than, the feasible distance (FD) of this router.

Feasible Distance (FD)

- The integer metric from the perspective of a this router.

Reported Distance (RD)

- Also, called Advertised Distance (AD).
- The integer metric from the perspective of a nexthop router.

Offset Lists

- Influencing the EIGRP metrics.

Successor

- Is the **best route, next-hop**, to a remote network (lowest cost).
- When EIGRP removes a successor route and no FS route exists, the router starts a process to discover if any loop-free alternative route exists to reach that prefix. This process is called **going active**.

Variance

- See **load-sharing/load-balancing**
- The variance is multiplied by the current **FD**.
- A **variance of 10** under the EIGRP process starts load balancing. 10 means that a metric up to 10 times greater than the best route metric will be allowed.
- **Equal-Cost load balancing** means only routes with the same lowest metric are installed in the local routing table.
e.g. `EIGRP maximum metric variance 1`
- Variance between **2** and **128** is used for **Unequal-Cost load balancing**.
- **Maximum path: 5** would indicate load balancing over max. 5 paths. The value can be from **1 to 16**. If the value is **1**, load balancing is disabled.

e.g.

```
router eigrp 100
variance 10
```

maximum-paths

- See load-sharing/load-balancing
- Default **4**
- Depending on the IOS **6** or **16**

Passive Mode

- When an interface is passive, EIGRP does not send any EIGRP messages on the interface -- multicast or EIGRP unicast - and the router ignores any EIGRP messages received on the interface.
- Redistributing of connected subnets is still possible.

Active Timer

- Default: **3 minutes**
- Routes for which a router does not receive a replay within the active time are **Stuck-in-Active (SIA)** routes.

Reasons for get in **Stuck-in-Active**:

- Bad or congested links
Flapping links?
- Query range is too long
- Router memory shortage


```
(config-router)#network 10.10.11.0 0.0.0.255 → Use Wildcard
```

```
(config)#router eigrp [ASN]  
(config-router)#address-family ipv4 autonomous-system 20  
(config-router)#network 172.16.0.0  
(config-router)#network 10.0.0.0
```

```
(config-router)#passive-interface [IF]  
(config-router)#neighbor 172.16.10.2  
(config-router)#variance 2 → Affects load balancing  
(config-router)#metric weights 0 1 0 1 0 0  
(config-router)#metric weights [tos 0-8] 0 1 0 1 0 0
```

```
(config-if)#no bandwidth → Reset BW to 1544 Mbps
```

Set the Hello-Interval in seconds

```
(config-if)#ip hello-interval [ASN] [sec]  
(config-if)#ip hello-interval eigrp 10 3
```

Set the Hold-Time in seconds

```
(config-if)#ip hold-time [ASN] [sec]
```

Set the router-id

```
(config-router)#eigrp router-id →
```

Advertising Static Default Routes with EIGRP

```
ip route 0.0.0.0 0.0.0.0 [IF] → Default route  
network 0.0.0.0 → Inject route to EIGRP topology database  
(config-router)#redistribute static →
```

Configuring a Default Network

```
(config)#ip default-network [x.x.x.x]
```

Make the router passive

```
router eigrp 1  
(config-router)#passive-interface fa0/0  
(config-router)#passive-interface default
```

```
no ip split-horizon eigrp [ASN] → See Frame Relay multipoint links  
ip bandwidth-percent eigrp [ASN] [%]  
offset-list [ACL] [in|out] [offset] [IF]
```

Configuring the Stub Router

```
(config-router)#eigrp stub  
(config-router)#eigrp stub connected summary → Connected & Summary enabled by default
```

```
timers active-time [time]  
ip prefix-list [x] ...  
(config)#route-map [NAME] [deny|permit] [x]  
(config-router)#distribute-list
```

Set Summarization

```
(config-if)#ip summary-address eigrp [ASN] [prefix] [subnet-mask]  
[no] auto-summary
```

Route Tag

```
(config)#route-tag notation dotted-decimal
```

Troubleshooting EIGRP

- ❑ Check **AS numbers**, must be equal

- Check interfaces
- Is an interface configured as **passive**?
- Are the interfaces enabled for EIGRP?
- Is the **IPv4 IF/Loopback** enabled?
- The **K values** must match (Default: K1=1, K2=0, K3=1, K4=0, K5=0)
- Is the EIGRP **authentication** misconfigured?
- Are the proper **networks** advertised?
- Is an **ACL** blocking the advertisement?
- Is **auto-summary** enabled
- Timers do not have to match **hello time/hold time**.
- Subnetmask** must match between peers.
- The neighbors must be in the **same subnet**.
- Keep in mind the **EIGRP event log** is always running.
- MTU** sizes doesn't have to match.

```
#show ip route                → Lists the EIGRP learned routes with a D.
#show ip route eigrp
#show ip protocols            → Shows the K-Values and passive interfaces and a
                               list of neighbor IP addresses

#show ip eigrp topology        → Lists all successor and feasible successor routes.
                               States P=passive, A=active
show ip eigrp topology active  →
#show ip eigrp topology all-links → Lists:
                               All possible next-hop IP addresses
                               Feasible successor routes
                               Non-feasible successor routes

show ip eigrp topology [Prefix] → e.g. 172.16.104.0/25
show ip eigrp topology pending →
show ip eigrp topology summary →

#show ip eigrp neighbors
#show ip eigrp neighbors detail → Shows:
                               Hello and Hold-time
                               Verifying stub settings
#show ip eigrp interfaces      → Lists the working interfaces on which EIGRP is
                               enabled. It omits passive interfaces

show ip eigrp interface detail [IF]
show ip eigrp events
#show ip eigrp traffic
show ip int brief

#show ip prefix-list
#show ip prefix-list detail    → Shows hits
#show ip prefix-list detail [route-map]

#show ip route tag             →
#show ipv6 route tag           →

#show protocols [IF]
#show route-map                → Statistics of matching packets.
                               Verifying the configuration.

(config-router)#eigrp log-neighbor-changes

#debug eigrp packets
#debug eigrp packet hello
#debug eigrp packet terse

#no debug all
```

EIGRPv6

- Supports **IPv6**
- EIGRP for IPv6 requires a **router ID**.
- Advanced distance-vector protocol with some link-state features.

- Multicast address **FF02::A**
- No **network** command is needed
- With IPv6, neighbor interfaces and next-hop addresses are **always link-local**.
- The **next-hop** is always the **neighbors link-local address**.
- EIGRPv6 advertises **IPv6 prefixes/lengths** rather than IPv4 subnet/mask
- EIGRPv6 cannot perform any **automatic summarization**.
- EIGRPv6 encapsulates its messages in **IPv6 packets**, rather than IPv4 packets.
- EIGRPv6 does not require neighbors to be in the **same IPv6 subnet** as a requirement to become neighbors.

Configuring EIGRPv6

```
(config)#ipv6 unicast-routing
(config)#ipv6 router eigrp [ASN]
(config-rtr)#no shutdown
(config-rtr)#router-id 1.1.1.1
```

```
(config-if)#ipv6 eigrp [ASN] → On each interface!
```

```
(config-if)#ipv6 summary-address eigrp [ASN] [ipv6-summary-route]
```

Troubleshooting EIGRPv6

```
show ipv6 eigrp interfaces
show ipv6 eigrp interfaces detail
#show ipv6 eigrp neighbors
#show ipv6 eigrp topology → Note: via connected and FD/AD networks
#show ipv6 eigrp topology all-links →
#show ipv6 protocols → Interfaces on which EIGRP is enabled
show ipv6 route → All routes
#show ipv6 route eigrp → All EIGRP learned routes
show ipv6 route [prefix/length] → Details

debug ipv6 eigrp notifications

#ping [ipv6] source loopback 0
```

Named EIGRP

Authentication: Supports **MD5** and **SHA authentication**.

- Named EIGRP consolidates disparate commands under a **single hierarchical structure**. This simplifies configuration and troubleshooting. That includes EIGRP for IPv4 and IPv6 router configuration mode and interface configuration mode.
- Traditional configured EIGRP routers can form a neighborhood with routers configured with Named EIGRP.
- The **autonomous-system** command is required for Named EIGRP!
- **Plain text authentication** and **PAP** is not supported by Named EIGRP.

Configuration Modes:

- **Address-Family**
e.g RID, network, eigrp stub, metric
#show run | s ospfv3 to view IPv4 and IPv6 configuration.
- **Address-Family-Interface**
e.g timer, passive interface, authentication, bandwidth-percent, hello-interval, hold-time, split-horizon
- **Address-Family-Topology**
e.g. variance, redistribute, auto-summary, maximum-paths

Service-Family and Service-Family-Interface

- For **Service Advertisement Framework (SAF)** feature like **Call Control Discovery (CCD)**.

Configuring Named EIGRP

```
(config)#router eigrp [virtual-instance-name]
(config-router)#address-family [ipv4|ipv6] autonomous-system [ASN]
(config-router-af)#network 0.0.0.0
(config-router-af)#af-interface [IF]
topology base
```

Define Global Setting for all IFs

- Can be overwritten by soecific IF setting.

```
(config-router-af)#af-interface [default|IF]
```

Troubleshooting Named EIGRP

```
s#how ipv6 eigrp interfaces
s#how ipv6 eigrp interfaces detail [IF]
#show ipv6 protocols → Interfaces on which EIGRP is enabled
#show ip eigrp topology
```

OPEN SHORTEST PATH FIRST (OSPF)

OSPFv2 IPv4
OSPFv3 IPv6

Transport: IP, protocol type **89** (does not use UDP or TCP)

Authentication: Supports **MD5** and **clear-text** authentication.

- **Link state protocol** for medium and large networks
- Must have an **area 0**
- Routers in one area must have the same **Link State - Database**.
- Routing-Protocol using the **Dijkstra** algorithm.
- Main purpose, **learning of IPv4-Routes**.
- Is working with **areas**, this reduces the processor calculation time and bandwidth consumption.
- Areas shouldn't contain more than **50** routers.
- Calculates the best route based on the **cost** of the outgoing interfaces.
- It supports **multiple, equal-cost routes** to the same destination, but does not support **unequal-cost** load balancing.
- It supports **VLSM/CIDR**.
- Multicast-Addresses used by OSPF **224.0.0.5** & **224.0.0.6**
- Does not support **auto-summary** (except at ABR routers)
- Max. number of **equal-cost paths** is **8**
- **Discover neighbors** before exchanging routing information's.
- In an **NBMA network**, such as Frame Relay, **no automatic discovery** is possible, therefore **manual configuration** of the neighbors is required.
- Uses a **hierarchical design** and is more complex to design as EIGRP
- Modern Cisco IOS versions typically support **16** or **32** concurrent routes to one destination.
- **No compatibility** between OSPFv2 and OSPFv3.
- Routes redistributed into OSPF have a default seed metric of **20**.
- The following Interface types are using a **DR/BDR**:
Broadcast, Nonbroadcast (NBMA)
- The following Interface types are **NOT** using a **DR/BDR**:
Loopback, Point-to-Point, Point-to-Multipoint, Point-to-Multipoint nonbroadcast.

Link

- Network or router interface assigned to any given network.

Router ID (RID)

- IP address to identify the router.
- 1. The **highest IP-Address** on any loopback interface is becoming the RID (Default)
- 2. **Highest logical interface** overrides a physical interface.
- 3. The **router-id** command overrides the interface and loopback interface.

Neighbor

- OSPF routers will become neighbors only if their interfaces share a network that's configured to belong to the same **area number**.
- The **process ID** must not match to become neighbors.
- A neighbor relationship needs:
Area ID
Stub area flag
Authentication password
Correct **Hello** and **Dead** intervals
`ip ospf hello-interval [sec]`

Adjacency

- Relationship between two OSPF routers.
- OSPF will only exchange routes with neighbors that also have established adjacencies.

Backbone Router

- Any router that has at least one interface connected to the backbone area

Internal Router

- A router that has interfaces connected to only one area, making the router completely internal to that one area

Designated Router (DR)

- DR assures that all Routers receive a copy of the LSAs.
- Generating LSAs representing the subnet and playing a key role in the database exchange process.
- Generates **Type-2** LSAs for the subnets.
- If the DR fails, the BDR becomes the DR and a new BDR will be elected.
- On **point-to-point** topologies, no DR will be elected
- **DROther** routers exchange their LSDB with the DR by sending the Type-2 message to **224.0.0.6**
- Setting the OSPF interface priority to a **value higher than 1** will influence the DR/BDR election in favor of the router.

Backup Designated Router (BDR)

- Is the hot standby for the DR.
- Receives all routing updates
- Does not disperse LSA updates
- If the BDR fails, a new BDR will be elected but the DR will remain unchanged.

DROther

- Also, called **Non-DR** router.
- Most likely seen in **broadcast networks**.

Hello Protocol

- Dynamic neighbor discovery by using multicast address **224.0.0.5**
- Sent every **10 seconds** by default.
- Contains: **RID, Hello/Dead interval, Neighbors, Area ID, Router priority, DR IP, BDR IP, Authentication data**

Network Type	Hello Interval (secs)	Dead Interval (secs)
Point-to-Point	10	40
Point-to-Multipoint	30	120
Broadcast	10	40
Non-Broadcast	30	120

Neighborhood Database

- List of all OSPF routers for which Hello Packets have been seen.

Link Statement Advertisement (LSA)

- Packet that contains link-state and routing information.
- Will only be exchanged when adjacencies are established.
- Exchanged with **LSU** messages
- The maximum number of LSAs learned by a router can be limited with **max-lsa [x]**
- LSA Type-1, Type-2 and Type-3 are not flooded **between areas**.

Area

- Grouping of **contiguous networks and routers**.
- A router can be a member of more than one area at a time
- There must be an **area 0**

Broadcast (multi access)

- A **DR** and **BDR** must be elected for each broadcast multi-access network.

Nonbroadcast Multi Access (NBMA)

- As its name suggests, a NBMA network **does not support broadcast**.
- **Frame Relay, X.25** and **ATM**
- Needs special OSPF configuration

- Can raise **Split Horizon** and **Designated router issues**.
- Recommended to use **point-to-point subinterface**.
- Sender must **know destination address** before sending packet.
- NBMA networks are either:
 - Hub and Spoke
 - Full-Mesh
 - Partial-Mesh

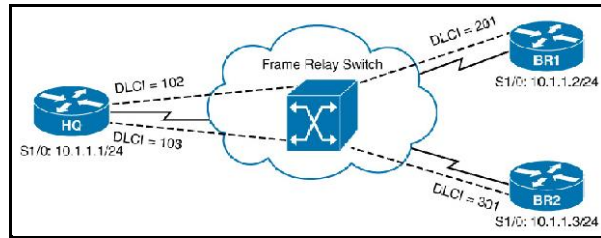


Figure 63: NBMA Network Type

Point-to-Point

- Eliminates the need of DRs or BDRs

Point-to-Multipoint

OSPF Metric Calculation

- See SPF

To influence the metric, you can:

- Change the Reference Bandwidth
(config-router) #auto-cost reference-bandwidth [bandwidth-Mbps]
- Set the interface bandwidth
bandwidth [speed]
- Set the OSPF cost directly
ip ospf cost [value]

Cost

- 1 - 65535
- Cisco uses $10^8/\text{bandwidth}$

Link Statement Database (LSDB) / Topological Database

- Storing topology data
- Contains information of all the Link State Advertisement packets that have been received.
- The existence of, and an identifier for, each router (router-ID)
- Each **router interface, IP address, mask** and **subnet**
- The list of routers reachable by each router on each interface
- LSDB exchange differs slightly if no DR exists

Virtual-Link

- An OSPF virtual link allows two ABRs that connect to the same nonbackbone area to form a neighbor relationship **through that nonbackbone area**, even when separated by many other routers and subnets.
- This virtual link acts like a **virtual point-to-point connection** between the two routers, with that link inside area 0
- See: **Do Not Age (DNA)** bit reduces overhead.
- **Hello/Dead** interval process is not used over virtual-links
- The **RID** in a virtual link is not pingable but the virtual link works

Pseudonode

- The pseudonode is a concept and not a router.
- The DR takes on the role of the Type-2 pseudonode

OSPF Network Types

- Broadcast

- Point-to-Point
- Loopback
- Nonbroadcast (NBMA)
- Point-to-Multipoint
- Point-to-Multipoint nonbroadcast

DD Packet (Database Description)

- Database Description packets are OSPF packet **Type-2**.
- These packets are exchanged when an adjacency is being initialized.
- They describe the contents of the link-state database.
- Multiple packets may be used to describe the database.
- For this purpose, a poll-response procedure is used.
- One of the routers is designated to be the master, the other the slave.
- The master sends Database Description packets (polls) which are acknowledged by Database Description packets sent by the slave (responses).
- The responses are linked to the polls via the packets' DD sequence numbers.

LSR-Packet (Link-State-Request)

- A packet that lists the LSIDs of LSAs that the sender of the LSR would like the receiver of the LSR to supply during database exchange.

LSU-Packet (Link-State-Update)

- A packet that contains fully detailed LSAs, typically sent in response to an LSR message.
- The name of the OSPF packet that holds the detailed topology information, specifically LSAs

LSAck Link-State Acknowledgment

- Sent to confirm receipt of an LSU message.

Area 0 = Backbone Area

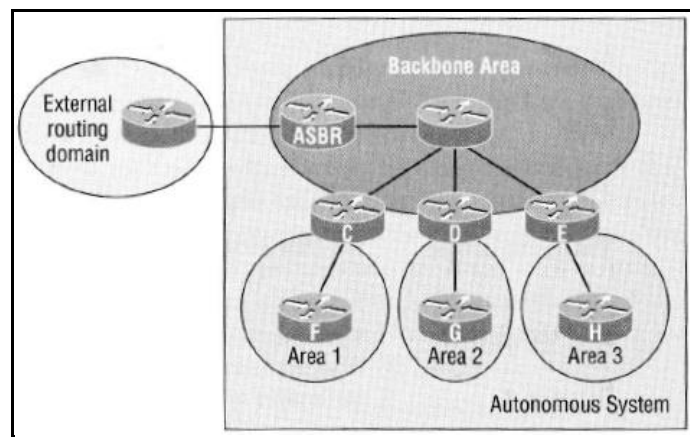
- All other routers must connect to area 0 except those connected via **virtual-link**.

Area Border Router (ABR)

- A router which connects other areas to the **backbone area** within an AS is called **ABR**
- This router has min. **2 interfaces**. One connecting to area 0 and the other to the other area.
- **ABRs** do not forward **Type-1** and **Type-2** LSAs from one area into another area.

Autonomous System Boundary Router (ASBR)

- A router which connects **ASs** (external networks).
- Creates **Type-5 External LSAs** for each redistributed subnet and lists the subnet number as the LSID.
- On the ASBR manual summarization can be performed `summary-address [prefix mask]`



OSPF-Router-ID negotiated during initialization of OSPF.

1. Neighbor and adjacency initialization

Sending of **OSPF-Hellos** (is there a neighbor / multicast 224.0.0.5)

My OSPF-Router-ID (RID) is

Frequency:

Broadcast and point-to-point every **10 sec** (Hello)

Non-Broadcast and point-to-multipoint every **30 sec**

2. LSA flooding

Share routing information via LSU packets.

Broadcast addresses:

Point-to-Point	224.0.0.5	All SPF Routers
Broadcast	224.0.0.6	All DR Routers
Point-to-Multipoint	NA	NA

Each recipient must acknowledge the **LSA**.

Default, every **30 min**.

3. Shortest Path First-Algorithm (SPF) - Calculation

- Calculation is based on the information collected in the **topology database (LSDB)** and the cost applied.

- Only changes to **Type-1** and **Type-2** require an SPF calculation.

- To calculate the **best route**, OSPF uses **Type-1**, **Type-2** and **Type-3** LSAs

- **Type-4**, **Type-5** and **Type-7** are used by OSPF to calculate routes for **external routes**.

The calculation steps are:

1. Analyze the LSDB to find all possible routes to reach the subnet.

2. For each route, add the OSPF interface cost for all outgoing interfaces in that route.

3. Pick the route with the lowest total cost.

Type-1-LSA

Router (Router Link States)

Router Description/Status

Router link advertisement (**RLA**).

Contains: Router ID (RID), interfaces, IP information & current interface status

Flooding: Stays within the area.

The LSDB contains one Type-1 LSA per router per area.

Uses a **32-bit** link-state identifier (LSID).

ABRs create multiple LSAs for themselves (one per area)

ABRs receive this LSA only from directly connected routers.

For **OSPFv3** the IP addressing semantic was removed.

Type-2-LSA

Network (Net Link States)

Network Description

Network link advertisement (**NLA**) created by **DRs**

Contains: DR and BDR IP information

Flooding: Stays within the area.

Created by the DR, one per transit network.

ABRs receive this LSA only from directly connected routers.

Remember: **Broadcast** and **Non-Broadcast** networks require a **DR/BDR**.

Database Description (**DD**) Packet

Type-3-LSA

Net Summary (Summary Net Link States)

Subnet Description (generated by ABRs) advertised in other areas.

Summary link advertisement (**SLA**) created by **ABRs**

Contains: ABR RID, IP and subnet mask

Flooding: **ABRs** are creating and flooding Type-3 LSAs into the next area.

"**O IA**" entries in the routing table represent a Type-3 LSA.

Type-4-LSA

ASBR Summary (Summary ASB Link States, OSPFv3)

Autonomous System Border Router (**ASBR**)

Are created by **ABRs**

Contains: Information how to reach the ASBR
 Flooding: Into all areas.

Type-5-LSA AS External
 External Routers injected into OSPF.
 External link advertisement created by **ASBRs**
 Fields: Metric, Mask, LSID, RID, External metric type (1 or 2 / "O E1" & "O E2")
 Flooding: Into all areas.
 Like a Type-3 LSA but for external routes.
 Not for stubby areas (NSSA's)
 Used by OSPF to represent each redistributed network.

Type-6-LSA Group Membership
 Deprecated: MOSPF
 Multicast OSPF-LSA
 Not supported by CISCO IOS
 Protocol Independent Multicast (PIM) is used instead.

Type-7-LSA NSSA External
 NSSA-LSA
 Created by **ASBRs** inside an NSSA area, instead of Type-5 LSAs

Type-8-LSA Link-LSAs (OSPFv3)
 Exists only on a local link, to advertise the router's link local address to all routers on the same link.
 Provides also a listing of all IPv6 addresses associated with the link.
 Local-link flooding scope, never flooded beyond the link with which they are associated.

Type-9-LSA Intra-Area Prefix-LSAs (OSPFv3)
 Can send information about IPv6 networks.
 Like the Type-1 and Type-2 LSA for IPv4 networks

Type-10,11-LSA Opaque
 Used as generic LSAs to allow easy future extension of OSPF.

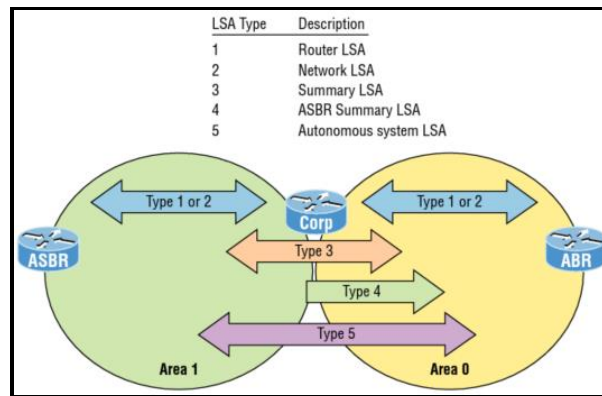


Figure 64: LSA Types

Stub network

- A network that has only **one entry and exit point**
- EIGRP defines **stub routers** as follows:
- For all types of stubby areas, the **ABR always filters Type-5 LSAs**
- For **"totally stubby"** and **"totally NSSA"** areas the ABR also **filters Type-3 LSAs**.
- **Totally stubby areas** contain only **Intra-area networks** and **Default route**.
- Commonly used in **hub** (distribution router) **and spoke** (remote router) **networks**.
- A stub router is a router that **should not forward traffic between two remote EIGRP-learned subnets**.

- In a hub and spoke topology, the remote router must forward **all nonlocal traffic to a distribution router**, so it becomes unnecessary for the remote router **to hold a complete routing table**.
- Generally, the distribution router need not send anything more than a **default route to the remote router**.
- The stub router responds to queries for summaries, connected routes, redistributed static routes, external routes, and internal routes with the message **"inaccessible"**.
- A **stub router** will send a special **peer information packet** to all neighboring routers to report its status as a stub router.
- Any neighbor that receives a packet informing it of the stub status will **not query the stub router** for any routes.

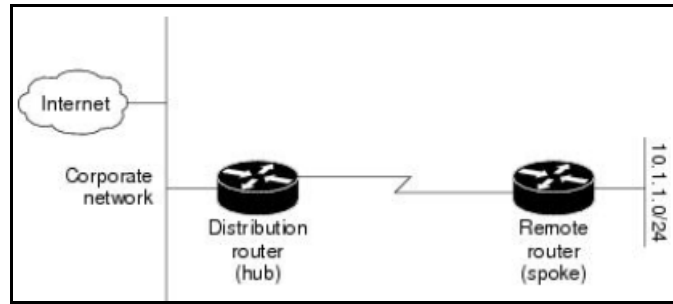


Figure 65: Hub and Spoke Network

Types of stubby areas:

- **stub** Does not accept external routes.
No Type-5 LSAs are allowed.
Type E1 & E2
- **totally stubby** (Cisco proprietary)
Does not accept external or inter-area routes.
Blocks Type-5, Type-3 and Type-4 LSAs
- **not-so-stubby (NSSA)**
See RFC 1587
Injection creates a LSA Type-7.
No Type-5 LSAs are allowed.
Limited capability to import external routes.
Type N1 & N2
Only **Type-1, Type-2, Type-3** and **Type-7** LSAs in the OSPF database.
- **totally NSSA** (Cisco proprietary)

Area Type	ABRs Flood Type 5 External LSAs into the Area?	ABRs Flood Type 3 Summary LSAs into the Area?	Allows Redistribution of External LSAs into the Stubby Area?
Stub	No	Yes	No
Totally stubby	No	No	No
NSSA	No	Yes	Yes
Totally NSSA	No	No	Yes

Figure 66: OSPF Stubby Area Types

Configuring STUB

```
(config-router)#area [x] nssa no-redistribution
```

Troubleshooting STUB

```
#show ip eigrp neighbors detail
```

→ Shows:
Verifying stub settings

Configuration NSSA

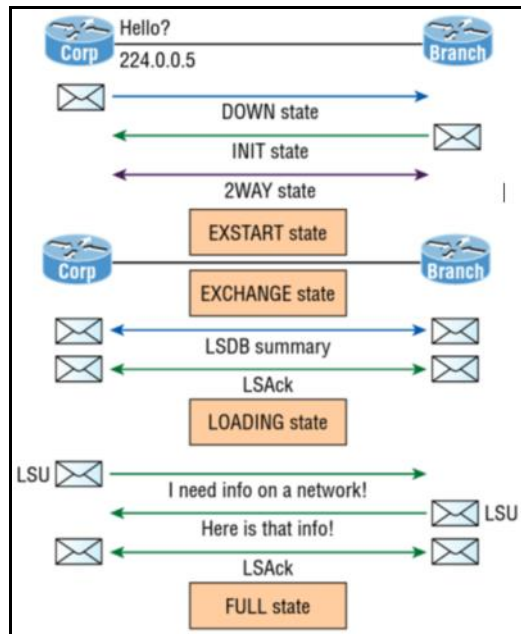
```
area [x] nssa
```

Configuration Totally NSSA

```
area [x] nssa no-summary
```

The OSPF Exchange Process

- EXSTART State
- EXCHANGE State
- LOADING State
- FULL State



Finite State Machine (FSM)

- 8 neighbor states to describe the current state of each neighbor.
- **DOWN**
- **ATTEMPT**
- **INIT** Permanent if the Hello parameters do not match
- **2-WAY** working neighbor that does not become fully adjacent.
- **EXSTART**
- **EXCHANGE**
- **LOADING**
- **FULL** state

OSPF Route Filtering

- Filtering Type-3 LSAs on ABRs
- Filtering Type-5 LSAs on ASBRs
- Filtering the routes that OSPF would normally add to the IP routing table on a single router

Type-3 LSA Filtering

- Type-3 LSA filtering tells the ABR to filter the advertisement of Type-3 LSAs.

```
router ospf
area [number] filter-list prefix [name] [in|out]
area [x] range [IP] [subnet] not-advertise    → Filter out Type-3 LSAs
```

```
-----
access-list [x] deny [IP] [subnet]
access-list [x] permit any
```

```
router ospf [x]
(config-router)#distribute-list [x] in
(config-router)#distribute-list prefix [x] in
```

Loopback Interfaces

- Loopback interfaces are logical interfaces.
- They ensure that an interface is always active and available for OSPF processes and are very handy for diagnostic- and configuration-purposes.
- The Loopback address with the highest IP-Address is becoming the **router ID**.

Configuring Loopback Interfaces

Create and Assign a loopback interface.

```
(config)#interface loopback 0           → Creates a loopback interface
(config-if)#ip address 1.1.1.1 255.255.255.255 → Assign loopback interface
```

Troubleshooting Loopback Interfaces

```

R1#show ip interface brief
Interface      IP-Address      OK? METHOD      Status          Protocol
FastEthernet0/0  10.1.0.1        YES NVRAM        up              up
FastEthernet0/1  unassigned      YES NVRAM        administratively down  down
Serial10/0/0     10.50.0.1       YES NVRAM        up              up
Serial10/0/1     10.51.0.1       YES NVRAM        up              up
Loopback0       1.1.1.1         YES unset       up              up

```

Figure 67: show ip interface brief

Wildcard Mask

- When configuring wildcards, they're always **one less than the block size**.
- The zeros (0) are representing the **matching bits in the IP address**.

```

/27      Block size 32  wildcard 31
/28      Block size 16  wildcard 15

```

Configuring OSPF

- Create the loopback interfaces before you enable OSPF routing!
- Enable OSPF by defining the **Process ID**
- Configuring OSPF areas

```

(config)#int loopback 0
(config-if)#ip address 172.31.1.1 255.255.255.255 → /32 saves subnets!

(config)#router ospf [processID]
(config)#router ospf 1
(config-router)#network 10.0.0.0 0.255.255.255 area [0] → Wildcard mask!
(config-router)#auto-cost reference-bandwidth 1000 → BW in Mbps
bandwidth [speed]
ip ospf cost [value]

```

```

(config-if)#ipv6 ospf 10 area 0           → IF configuration
(config-if)#ipv6 ospf cost [x]           → Change the cost of a route
passive-interface Fa0/0                    →

```

```

ip ospf dead-interval minimal hello-multiplier [multiplier]
(config-if)#ip ospf network non-broadcast

```

Route Summarizations on ABRs

```
(config-router)#area [x] default-cost [x]
(config-router)#area [x] nssa
  (config-router)#area [x] range [0.0.0.0 0.0.0.0] [cost] → Influence Type-3 LSAs
(config-router)#area [x] stub
(config-router)#area [x] stub no-summary
(config-router)#area [x] virtual-link [IP]

(config-if)#ip ospf priority [1-255] → To modify the OSPF priority
(config-if)#ip mtu 1400
summary-address [prefix mask] → Used on ASBRs for summarization
```

Inject a default route

```
(config-router)#default-information originate
```

Creates a totally stubby area

```
(config-router)#area [x] nssa [no-summary]
```

Filtering Type-3 LSAs

```
(config)#ip prefix-list FILTER-AREA-51 seq 5 deny 192.168.1.0/24
(config)#ip prefix-list FILTER-AREA-51 seq 10 permit 0.0.0.0/0 le 32
```

Modify the default OSPF external-type

```
set metric-type type-1
```

Filter routes, not LSAs before adding them to the routing table

```
(config-router)#distribute-list in
```

Troubleshooting OSPF

- Hello** and **dead timers** must match
- Area ID** and type must match
- Subnet** must match
- Authentication** data must match (if used)
- Check **adjacencies**
- Cost** must match
- K-values** must match
- Check conflict with **Router-IDs** (must be unique)
- Check the **MTU** values
- The **process ID** must not match
- Check **Stub area flag**
- List of neighbors reachable on the interface
- Router priority
- DR and BDR IP address

```
show ip interface brief →
show ip interface [x] →

show ip ospf → Number of SPF runs
#show ip ospf | begin Area → Number of SPF runs

show ip ospf neighbor → Lists know neighbors and neighbor state
show ip ospf neighbor [IF] →
#show ip ospf neighbor detail [IP] →

#show ip ospf interface [x] → Hello, Dead timer and MTU (Must Match!)
Authentication type, BW, Cos30
#show ip ospf interface brief → Lists the interfaces on which OSPF is enabled.
Omitting passive interfaces.

show ip ospf interface neighbor [x] →

#show ip ospf database → Shows the collection of OSPF link states
Lists a single line for each LSA
#show ip ospf database asbr-summary → Type-4 LSAs
```

```

#show ip ospf database asbr-summary [RID]

#show ip ospf database external          → Type-5 LSAs
#show ip ospf database external [IP]

#show ip ospf database network [IP]

#show ip ospf database router            →
#show ip ospf database router [RID]     →
#show ip ospf database router self-originated

#show ip ospf database summary           → Lists only Type-3 LSAs
#show ip ospf database summary [IP]

show ip ospf database database-summary
show ip ospf database nssa-external
show ip ospf database nssa-external [x]

show ip ospf border-routers

#show ip ospf route                      → Shows Interarea and Intra-Area routes

#show ip route                           →
#show ip route ospf                      →
#show ip prefix-list                     →

#show ipv6 route                         →
#show ipv6 protocols                     → Lists the interfaces on which OSPF is enabled.
#show ipv6 ospf interface [x]           →

#show ip ospf virtual-links              →

debug ip ospf hello                      →
#debug ip ospf adj                       →

```

```

R1>show ip ospf
Routing Process "ospf 10" with ID 10.51.0.1
Start time: 17:20:26, Time elapsed: 00:04:38
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Link-local Signaling (LLS)
Supports area transit capability
Router is not originating router-LSAs with maximum metric
Initial SPF schedule delay 5000 msec
Minimum hold time between two consecutive SPF's 10000 msec
Maximum wait time between two consecutive SPF's 10000 msec
Incremental-SPF disabled
Minimum LSA interval 5 secs
Minimum LSA arrival 1000 msec
LSA group pacing timer 240 secs
Interface flood pacing timer 33 msec
Retransmission pacing timer 66 msec
Number of external LSA 0. Checksum Sum 0x000000
Number of opaque AS LSA 0. Checksum Sum 0x000000
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
Number of areas transit capable is 0
External flood list length 0
  Area BACKBONE(0)
    Number of interfaces in this area is 3
    Area has no authentication
    SPF algorithm last executed 17:20:27 ago
    SPF algorithm executed 5 times
    Area ranges are
    Number of LSA 2. Checksum Sum 0x008AC0
    Number of opaque link LSA 0. Checksum Sum 0x000000
    Number of DCbitless LSA 0
    Number of indication LSA 0
    Number of DoNotAge LSA 0
    Flood list length 0

```

```
R3#show ip ospf neighbor
Neighbor ID Pri State Dead Time Address Interface
10.51.0.1 0 Full/ 00:00:39 10.51.0.1 Serial0/0/0
10.52.0.1 0 Full/ 00:00:39 10.52.0.1 Serial0/0/1
```

Figure 68> show ip ospf neighbor

OSPFv3

RFC 5340, 2740

Authentication: OSPF supports **MD5 authentication** and **plaintext authentication** leveraging **IPSec**.

- OSPFv3 is still a **link-state routing protocol**.
- OSPFv3 still uses **multicast traffic** to send its updates and acknowledgments, with the address **FF02::5** for OSPF routers and **FF02::6** for OSPF-designated routers. These new addresses are the replacements for **224.0.0.5** and **224.0.0.6**.
- Networks attached are configured in **interface mode**.
- It supports **multiple IPv6 subnets** on a single link
- It routes over **links** rather than over networks (OSPFv2)

Renamed LSAs:

- Type-3 Interarea prefix LSA for ABRs
Generated by ABRs
- Type-4 Interarea router LSA for ABRs
How to reach an aASBR

```
(config)#ipv6 router ospf 10
(config-router)#router-id 1.1.1.1
```

```
ipv6 ospf 10 area 0
```

OSPFv3 Address Family Configuration

- Does not peer with OSPFv2.

```
router ospfv3 [process-id]
router-id                               → Optional
address-family [ipv4|ipv6] unicast
(config-if)#ospfv3 [process-id] [ipv4|ipv6] area [x]
```

Configuring OSPFv3

- Enable IPv6 unicast routing (even if you don't use IPv6)
- Start the OSPF process
- Configure a router ID (Optional)
- Instruct one or more interfaces to participate in the OSPF routing process

```
(config)#ipv6 unicast-routing
```

```
(config)#interface f0/0
(config-if)#ipv6 address 2001:db8:3c4d:11::/64 eui-64
...
copy run start
```

```
show ipv6 route
```

```
-----
(config)#int f0/0
(config-if)#ipv6 ospf 1 area 0
(config)#int s0/0
-----
```

```
#show ipv6 route ospf
#show ipv6 protocols
```

→ Lists the interfaces on which OSPFv3 is enabled.

```
----- CHANGE THE RID
(config)#ipv6 router ospf 1
(config-router)#router-id 1.1.1.1
#clear ip ospf [process]
```

```
(config-if)#ip ospf cost [1 - 65535]
```

```
summary-address 128.213.96.0 255.255.254.0
```

```
passive-interface [Loopback0]
```

→ Prevent unnecessary OSPF msgs out of this interface

```
frame-relay map
```

→ For IPv6 over Frame Relay

```
are [x] stub no-summary
```

Troubleshooting OSPFv3

```
show ipv6 ospf
```

```
#show ipv6 ospf database
```

```
show ipv6 ospf int [IF]
```

```
show ipv6 ospf int brief
```

```
show ipv6 ospf neighbor
```

```
#show ipv6 protocols
```

→ Lists the interfaces on which OSPFv3 is enabled.

```
#show ipv6 route ospf
```

→ O = Intra-Area / OI = Inter-Area (different)

```
show ip interface brief
```

```
show ipv6 interface brief
```

```
show ospfv3 database
```

```
#show ospfv3 interface brief
```

```
#show ospfv3 neighbor
```

```
debug ipv6 ospf packet
```

```
debug ipv6 ospf hello
```

MULTI-AREA OSPF

- OSPF **converges** much faster than RIP.
- **Topology changes** in one area won't cause global OSPF recalculations.
- **Routing tables** will be much smaller than in on global area.
- **Routers exchange LSAs** and learn the complete topology of the network until all routers have the exact same topology database.
- OSPF uses **Dijkstra algorithm** to find the best path to each remote network.

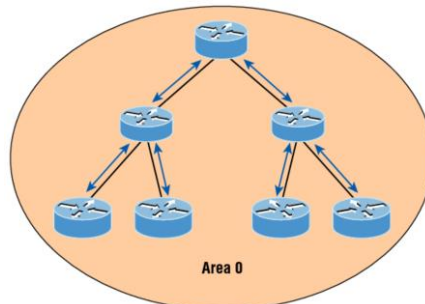


Figure 69: OSPF single area

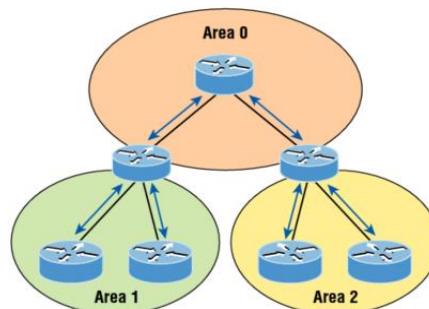


Figure 70: OSPF multi area

Adjacency Requirements

1. Two-way communication with **Hello**
2. **Database synchronization**
DD-Packets (Database description)
LSR-Packets (Link-State Request)
LSU-Packets (Link-State Update)
3. To build **adjacency**, the following must match:
Area ID
Subnet
Hello and dead timers
Authentication (if configured)

Configuring Multi-Area OSPF

```
(config)#router ospf 1
(config-router)#router-id 1.1.1.1      → RID must be different on each router
(config-router)#network 10.10.0.0 0.0.255.255 area 0
(config-router)#network 172.16.10.0 0.0.0.3 area 1
(config-router)#network 172.16.10.4 0.0.0.3 area 2
```

```
(config-router)#auto-cost reference-bandwidth [1-4294967]
(config-if)#ip ospf cost 10
```

```
area [x] range [IP] [subnet] not-advertise    → Filter out Type-3 LSAs
```

Troubleshooting Multi-Area OSPF

```
#show ip interface brief          →
#show ip interface [x]           →
#show ip ospf                    →
#show ip ospf neighbor           → Shows RID, are info, SPF stat, LSA timer
#show ip ospf interface [x]      → Shows Hello and Dead timer (Must Match!)
#show ip ospf interface brief    →
#show ip ospf interface neighbor [x] →
#show ip ospf database           →
#show ip route                   →
#show ip route ospf              →
#show ipv6 route                 →
#show ip protocols                →

#debug ip ospf hello             →
```


BORDER GATEWAY PROTOCOL (BGP)

RFC 1771, 827, 904

Transport: BGP relies upon communication over **TCP port 179**.

Tools: <http://routerserver.org/> Public Route Servers

"Not as many internetworks need BGP as you might think"
Jeff Doyle, Book: Routing TCP/IP Volume II

Versions:

BGP version 4 (BGP-4, RFC 4760)

- It supports only routing of **IPv4 networks**.
- It uses **Network Layer Reachability Information (NLRI)** between routers to carry supernetting information, as well as perform aggregation.
- **BGP** is a **distance-vector** protocol (Path vector protocol).
- **BGP** connects **autonomous systems (AS)** together.
- Is used between **Internet Service Providers (ISPs)** to exchange the Internet's routing table.
- **BGP** obsoletes **EGP**
- **BGP** gives engineers many ways to influence BGP's **best-path selection**.
- BGP uses **Path Attributes (PAs)** to influence the selection of the best path (path vector).
- Exterior Gateway Protocol (**EGP**)
- The fact, that all OSPF areas must be connected to **area 0** simply doesn't allow to scale OSPF as replacement for BGP
- Furthermore, OSPF does not have any mechanism to **modify path selection** based upon factors such as interconnection agreements between ISPs.
- BGP enforces the rule that no **AS path list** can contain the same AS number twice
- **BGP** neighbors exchange updates on a **triggered basis** and monitor their connection state via **periodic keepalives**
- There is no requirement that every **eBGP** router be a **neighbor** to every other eBGP router
- BGP uses the **AS_PATH** to perform two key functions:
 - Choose the best route for a prefix based on the shortest AS_PATH
 - Prevent routing loops
- The single **biggest reason** to consider using BGP between an enterprise and an ISP is to influence the choice of best path/route.
- If you've **multiple @Internet connections**, and you want to influence some packets to take one path and some packets to take another, consider BGP.
- BGP does not use the `network` command to enable BGP on interfaces. In fact, **BGP has no concept of being enabled on interfaces**.
- Enterprises that choose to use BGP benefit from both **learning routes** from the connected ISPs and **advertising** the enterprise's public prefix to the same ISPs.
- **BGP** forms a neighbor relationship **before** sending routing information.

ISPs give you three BGP options:

- **Default route only**
The ISP advertises a default route with BGP, but no other routes.
- **Full updates**
The ISP sends you the entire BGP table.
- **Partial updates**
The ISP sends you routes for prefixes that might be better reached through that ISP, but not all routes, plus a default route.

BGP Synchronization

- A BGP router should not advertise to external neighbors, destinations learned from inside BGP neighbors unless those destinations are also known via IGP.

BGP Neighbor States

Idle	Refuses connections Routing table being searched to check the neighbor reachability.
Connect	Waits for the connection to be completed Connect retry timer = ?
OpenSent	Waits for an OPEN message The 3-Way TCP handshake was successful.
Active	Listens for and accepts connections Means BGP has given up building the 3-Way TCP handshake. No response to the open message has been received within 5 seconds. The neighbor is peering with the wrong address. There is no neighbor statement for the peer. There is no route to the source IP address of the BGP open packet.
OpenConfirm	Session parameter negotiation completed Waits for a KEEPALIVE or NOTIFICATION message
Established	Sending BGP Update messages to each other <code>show ip bgp summary</code> → State/PfxRcd shows a number

BGP Message Types

- Size: 19 to 4096 octets.
- BGP Header = 19 octets.

1	Open	
2	Update	
3	Notification	
4	Keepalive	(Default 60 sec)

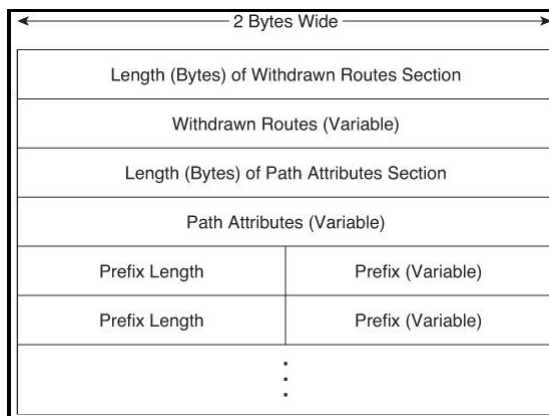


Figure 71: BGP Update Message

BGP Table

- The BGP Table should hold all learned prefixes, from each neighbor, except for any prefixes filtered by an inbound BGP filter (see `neighbor route-map in` command).
- BGP configuration does not allow filtering of all **inbound** or **outbound updates**. Instead the BGP filtering configuration enables filters **per neighbor**.

Discard Route

Also, called null static route

BGP Transit AS

- Anytime you are allowing **an AS that you do not control**, to access another AS that you do not control, via your BGP AS (aka, by traveling through your network), then you are a **transit AS**.
- A BGP transit autonomous system is an AS that allows full internet traffic to pass through it. This is traffic that neither originated from nor is destined to an AS you control. It's just "passing through"

your AS. Some organizations have a need for BGP, but don't want to allow internet traffic to flow through their AS. I guess we could call that a stub AS?

iBGP - Internal BGP

- **BGP** neighbors in the **same AS** are referred as **internal BGP (iBGP)**
- **iBGP** routers must be configured as a neighbor **to every other iBGP router in the same area**, to prevent routing loops.
- **iBGP** updates goes only **one hop** to prevent iBGP loops.
- When advertising a route to an **iBGP** peer, the advertising router **does not change the next-hop address**.
- Updates from iBGP peers do include the **Local_Pref PA**.
- iBGP **confederations** solves iBGP mesh problems.
- **iBGP** does NOT add its own ASN to the AS_PATH PA before sending routing information to another router.
- **iBGP neighbors** need to be in a **full mesh** of peers.

When an enterprise uses more than one router to connect to the @Internet, and those routers use **BGP** to exchange routing information with their **ISP**, those same routers need to exchange BGP routes with each other as well. The BGP neighbor relationships occur inside that enterprise, - inside a single ASN - making these routers iBGP peers.

Configuring iBGP

- The **neighbor** command lists same ASNs, making the routers to iBGP peers.
- You may change the **iBGP** behavior with the `neighbor [neighbor-ip] next-hop-self` command.

```
#neighbor [neighbor-ip] next-hop-self →  
#bgp asnotation dot → Changes the default display format of the ASN  
#no bgp asnotation dot →
```

Troubleshooting iBGP

```
#show ip interface brief  
#show ip protocols  
#show ip bgp → Shows the entire BGP table.  
#show ip bgp summary  
#show ip bgp neighbor → Phrase <internal link> indicates the neighbor is in the same  
ASN. <external link> would indicate, it would be an eBGP peer.  
#show ip route bgp
```

eBGP - External BGP

- **eBGP** means the routers are in **different ASNs**.
- If you're configuring BGP **between a customer network and an ISP**, this process is called external BGP (EBGP).
- By **default**, when a router advertises a route using **eBGP**, the advertising router lists its **own update-source IP address** as the next-hop IP address of the route.
- **eBGP** neighbors must be **directly connected**.
- **eBGP** adds its own ASN to the AS_PATH PA before sending routing information to another router.

Configuring eBGP

1. Define the BGP process
2. Establish one or more neighbor relationships
3. Advertise the local networks into BGP
4. Use the **ebgp-multihop command** if the eBGP peer is no directly connected.

```
(config)#router bgp [ASN] → ASN 1 - 65'535  
(config-router)#neighbor 192.168.1.2 remote-as 100
```

```
...
(config-router)#network 10.0.0.0 mask 255.255.255.0
```

```
-----
bgp router-id [rid]
neighbor [neighbor-ip] password [key]
neighbor [neighbor-ip] remote-as [ASN]
[no] neighbor [neighbor-ip] shutdown
neighbor route-map in
```

```
-----
aggregate-address [IP] [SN] summary-only
-----
```

To build a neighborhood with a not directly connected router.
- Default 255 hops

```
neighbor [neighbor-ip] ebgp-multihop [hops]
```

To tell BG which IF should answer hello packets.

```
neighbor [neighbor-ip] update-source [IF]
```

Configure load balancing with BGP:

```
maximum-paths [2]
maximum-paths ibgp [2]
```

Configure peer-groups:

```
neighbor [IP] peer-group [name]
neighbor [name] peer-group [nlri] [unicast|multicast]
```

Configure confederations:

```
bgp confederation identifier [ASN]
bgp confederation peers [x] [y]
```

Troubleshooting eBGP

```
#show ip interface brief
#show ip protocols
#show ip bgp
#show ip bgp summary
#show ip bgp neighbor
#show ip route bgp
```

```
debug ip bgp
```

Single-Homed (1 link per ISP, 1 ISP)

Dual-Homed (2+ links per ISP, 1 ISP)

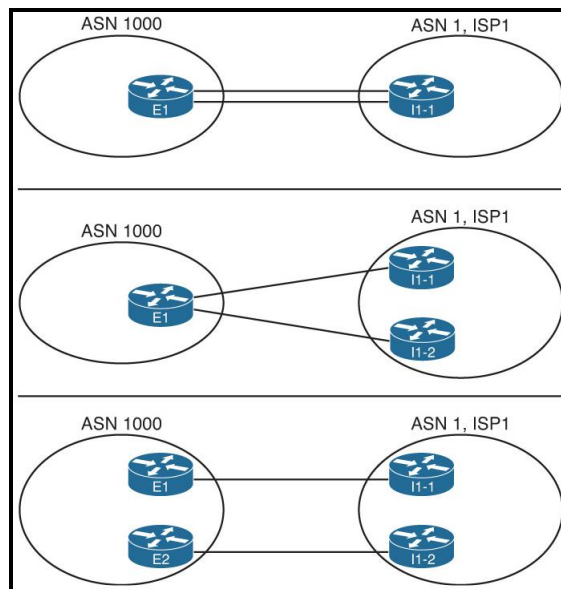


Figure 72: Dual-Homed Design Options

- To prefer one @Internet connection over another for all destinations, but when the better ISP connection fails, all traffic reroutes over the secondary connection.
- To treat both @Internet connections as equal, sending packets for some destinations out each path, However, when one fails, all traffic reroutes over the one still-working path.

Single-Multihomed (1 link per ISP, 2+ ISPs)

- **AS_PATH** is used to influence inbound path selection.
- **LOCAL_PREF** is used to influence outbound path selection.

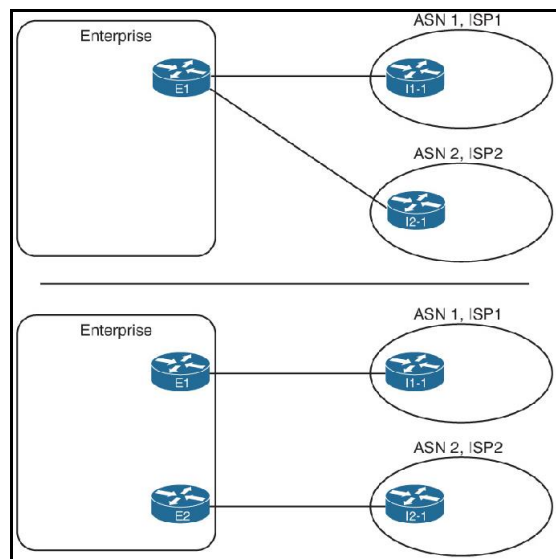


Figure 73: Single-Multihomed Designs

Dual-Multihomed (2+ links per ISP, 2+ ISPs)

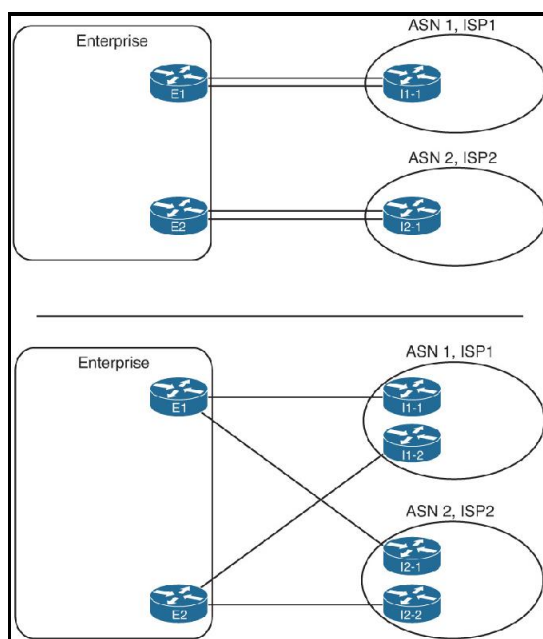


Figure 74: Dual-Multihomed Options

BGP Path Attributes (PA)

- BGP Path Attributes define facts about a particular route or path through a network.
- After the best path is calculated, the router gives the best route to another process, the **Cisco IOS Routing Table Manager (RTM)**.

Decision Steps

0 Next_Hop PA

List's the next-hop address to reach a prefix.
well-known mandatory attribute.

1 Weight

0 - 65'535 can only be set on input.
Cisco specific.
Assigned locally on the router.
The value is not propagated in any UPDATE message.
Default: 32768
Higher weights are preferred.
neighbor route-map in
neighbor [IP] weight [value]

2 Local_Pref

0 - 2^{32} route preference
well-known discretionary attribute.
Not included in eBGP updates but in iBGP updates.
iBGP **default 100**
Higher Local_Pref the better route.
Can be set by neighbor [IP] route-map.
Often used to influence outbound path selection.

4 AS_Path

The number of ASNs in the AS_Path PA.
well-known mandatory attribute.
Primary loop-prevention tool.
Used to calculate the AS_Path length.
Most common reason for path selection.
AS-Path filters use regular expressions.
AS_Path prepend can be used to influence inbound and outbound routing.

- 5 Origin About injection
well-known mandatory attribute.
0 = IGP
1 = EGP (obsolete)
2 = incomplete

- 6 MED Multi-Exit Discriminator
optional and nontransitive attribute.
Smallest-is-best logic.
ISP Engineers typically use MED when advertising an enterprise's public IP address space.
0 - 2^{32} can be set
Default = 0
set metric [x]

- 7 Prefers eBGP routes over iBGP routes.

- 8 Lowest IGP Lowest IGP metric to the next hop.

- 9 Lowest Router_ID Lowest Router_ID

- 10 Shortest Cluster-List Client must be aware of RR attributes.

- 11 Lowest neighbor IP Lowest neighbor IP address.

- ATOMIC_AGGREGATE **well-known discretionary** attribute.

- AGGREGATOR **optional transitive** attribute.

- COMMUNITY **optional transitive** attribute.

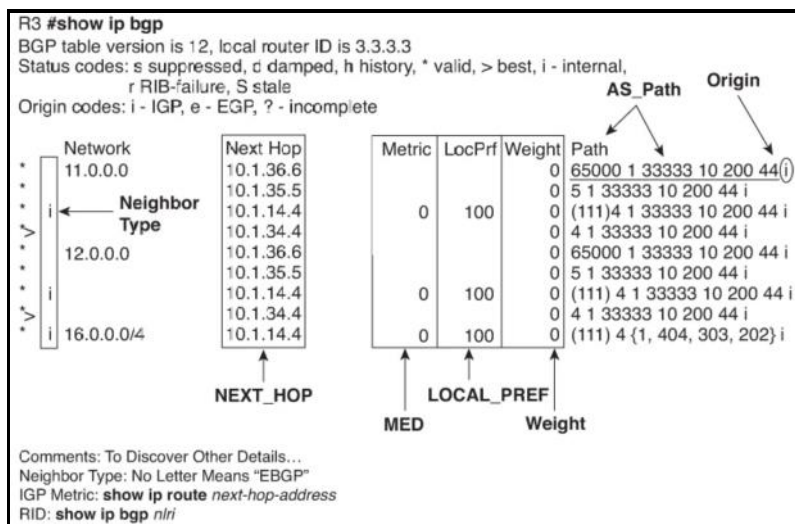


Figure 75: Find BGP PA Settings

Step	Mnemonic Letter	Short Phrase	Which Is Better?
0	N	Next hop: reachable?	If no route to reach Next_Hop, router cannot use this route.
1	W	Weight	Bigger.
2	L	Local_Pref	Bigger.
3	L	Locally injected routes	Locally injected is better than iBGP/eBGP learned.
4	A	AS_Path length	Smaller.
5	O	Origin	Prefer I over E. Prefer E over ?
6	M	MED	Smaller.
7	N	Neighbor type	Prefer eBGP over iBGP.
8	I	IGP metric to Next_Hop	Smaller.

Figure 76: BGP Decision Process (N WLLA OMNI)

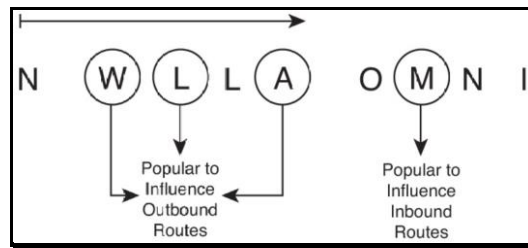


Figure 77: Influencing Best Path

Peer Groups

- Cisco IOS allows you to logically group similar neighbors into a **BGP peer group**.
- You may apply nondefault BGP configurations to the peer group, this can dramatically decrease the required CPU resource.

Configuring BGP

```
(config)#router bgp [ASN]                → ASN 1 - 65'535
(config-router)#neighbor 192.168.1.2 remote-as 100
(config-router)#neighbor 192.168.1.2 update-source loopback0
(config-router)#neighbor 192.168.1.2 next-hop-self
...
(config-router)#neighbor [IP] description [TEXT]
...
(config-router)#network 10.0.0.0 mask 255.255.255.0
-----
bgp router-id [rid]
neighbor [neighbor-ip] password [key]
neighbor [neighbor-ip] update-source [IF]
neighbor [neighbor-ip] ebgp-multihop [hops]
[no] neighbor [neighbor-ip] shutdown
neighbor [neighbor-ip] soft-reconfiguration
neighbor [neighbor-ip] soft-reconfiguration inbound
neighbor [neighbor-ip] shutdown
-----
aggregate-address [IP] [SN] summary-only
[no] synchronization                → See transit networks
neighbor distribute-list
neighbor [IP] distribute-list [ACL] out

neighbor prefix-list
neighbor [IP] prefix-list only-public

neighbor filter-list

neighbor route-map in
neighbor route-map [x] in

ip prefix-list ONLY-PUBLIC permit [prefix]
```



```

ip prefix-list NAME permit [prefix] ge 24 le 24
ip prefix-list STD-GATEWAY permit 0.0.0.0/0

set weight [x]
set local-preference [x]
set as-path prepend 3 3

```

Quickly set the WEIGHT

```
(config-router)#neighbor [IP] weight [x]
```

--- Hard reset-----

```
clear ip bgp *
clear ip bgp [IP]
```

--- Soft reset or Route Refresh -----

```
clear ip bgp * soft
clear ip bgp [IP] soft
clear ip bgp [IP] out|in          → Soft reset
clear ip bgp [IP] soft out|in
```

--- BGP Peer Group -----

```
neighbor [ROUTE-PG] peer-group
neighbor [ROUTE-PG] prefix-list [ROUTE-DEMO] in
```

--- Filtering -----

```
router bgp [ASN]
neighbor [ROUTE-PG] distribute-list [x] in
access-list [x] deny [IP/WC]
access-list [x] permit any
```

--- Filtering -----

Per neighbor.

```
(config)#ip as-path access-list [x] [permit|deny] [regex]
(config-router)#ip as-path access-list [x] permit .*
```

--- Route Reflector -----

```
#neighbor [IP] route-reflector-client
```

--- Graceful restart -----

```
#neighbor [IP] ha-mode graceful-restart
```

--- SET WEIGHT -----

```
(config-router)#neighbor [IP] weight [0-65'535]
#clear ip bgp peer-group *
```

--- SET LOCAL PREFERENCE -----

```
(config)#route-map [NAME] permit 10
(config-route-map)#set local-preference 150 → Higher = Better
(config)#router bgp [ASN]
(config)#neighbor [IP] route-map [NAME] in
#clear ip bgp [IP]
```

Troubleshooting BGP

- Is authentication configured?
- Ensure that each router can reach the *next-hop address* listed in the BGP routes.

```
#show ip as-path-access-list [filter list]
```

```
#show ip protocols          →
#show ip route              →
#show ip int brief          →
```

```
#show ip bgp                →
#show ip bgp summary        →
#show ip bgp neighbors      →
```

```

#show ip bgp x.x.x.x.                →
#show ip bgp 0.0.0.0 0.0.0.0        → List possible default routes
#show ip bgp [prefix] [subnet-mask] → Possible routes per prefix
#show ip bgp neighbors [ip] routes
#show ip bgp neighbors [ip] received-routes
#show ip bgp neighbors [ip] advertised-routes

#show ip bgp regexp [regex]
#show ip bgp filter-list [ACL-number]

#show ip bgp rib-failures

#show tcp brief                      →

#clear ip bgp                        →
#clear ip bgp [ASN]                 →

#debug ip bgp ipv4 unicast

```

Multiprotocol BGP (MP-BGP)

- Is the **update to BGP-4** and supports multiple address types.
- Supports routing for **IPv6 networks**, **next hop** attribute and **NLRI** is in IPv6 format.
- Traditional **BGP-4 router** can form a neighborhood with an MP-BGP router.
- For **IPv6 filtering** you can use:
Filter-Lists, Prefix-Lists and Route-Maps

Supported Address Families (not complete):

- Unicast IPv4
- Multicast IPv4
- Unicast IPv6
- Multicast IPv6
- Virtual Private LAN Service (VPLS)
- Layer 2 VPN (L2VPN)

New Features:

- Address Family Identifier (AFI)
- Subsequent Address Family Identifier (SAFI)
- Multiprotocol Reachable Network Layer Reachability Information (MP_REACH_NLRI)
- Multiprotocol unreachable Network Layer Reachability Information (MP_UNREACH_NLRI)
- BGP Capabilities Advertisement

Configuring MP-BGP

IPv6 over IPv4 BGP Session:

```

(config)#ipv6 unicast-routing
route-map [x]
set ipv6 next-hop [IPv6]
router bgp [ASN]
neighbor [IP] remote-as [ASN]
address-family ipv4
network [ipv4] [mask]
exit-address-family
address-family ipv6
network [ipv6] [prefix]
neighbor [IP] activate
neighbor [IP] route-map [route-map-name] out

```

IPv6 over IPv6 BGP Session:

```

(config)#ipv6 unicast-routing
router bgp [ASN]
neighbor [IP] remote-as [ASN]
address-family ipv6

```

```
network [ipv6] [prefix]
neighbor [IP] activate
```

Troubleshooting MP-BGP

```
show ipv6 route
show bgp ipv6 unicast
show bgp ipv6 unicast summary
```

WIDE AREA NETWORKS (WANs)

Definition of a WAN:

- Distance factor.
- Typically leasing from a service provider.
- You don't own it.

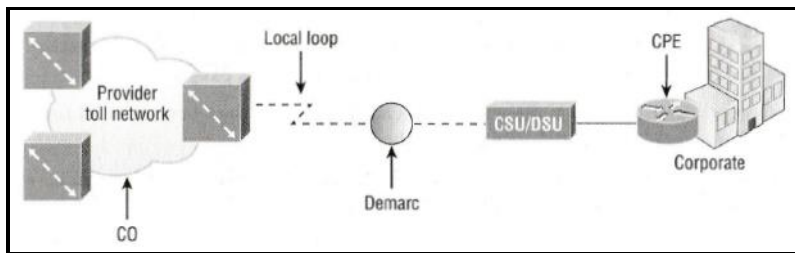


Figure 78: WAN Terms

Demarcation Point

- Where the **service provider's responsibility ends** and the CPE begins.
- It's your responsibility to cable from this box to the CPE, which is usually a connection to a CSU/DSU. More recently we see the provider giving us an Ethernet connection.

Local Loop

- Connects the Demarc to the closest switching office, referred to as the central office.

Central Office (CO)

- This point connects the customer's network to the provider's switching network.

Toll Network

- Is a **trunk link** inside a WAN provider's network.
- A collection of switches and facilities owned by the ISP.

Customer Premises Equipment (CPE)

- Any equipment related to communications that is located at the customer site, as opposed to inside the telephone company's network.
- Typically owned by the subscriber and located on the subscriber's premises.

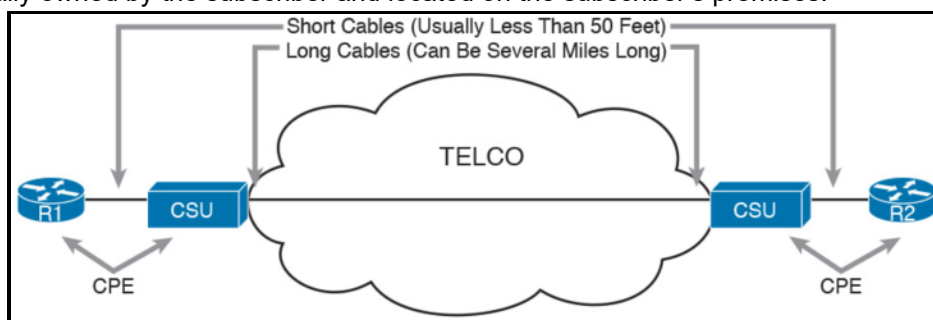


Figure 79: CPE and CSU

Channel Service Unit (CSU) / Data Service Unit (DSU)

A device that understands the Layer 1 details of serial links installed by a telco and how to use a serial cable to communicate with networking equipment such as routers.

WAN Connection Bandwidth

DDS Lines

- Transmission Rate 2.4 to 56 Kbps
- Point-to-Point
- Dedicated point-to-point connections with guaranteed full-duplex bandwidth and nearly error-free communication paths. DDS sends data from a router/bridge over a Channel Service Unit/Data

Service Unit, which converts standard computer digital signals to bipolar signals used in synchronous communications.

Digital Signal 0 (DS0)

- Basic signaling rate of 64 Kbps.
- E0 = Europe
- J0 = Japan
- 1 DS0 = 1 voice/data line

T1 (DS1)

- T1 comprises 24 DS0 circuits bundled
- 1'544 Mbps
- Full-Duplex
- Point-to-point
- Also referred as DS1
- T1 sends voice, data, and video over two-wire pairs with a full-duplex signal. One pair of wires sends, and the other pair receives. Due to the cost of T1 lines, some clients use fractional T1 lines that provide them with 64 Kbps channels incrementally, according to demand.
- T1 lines use a form of multiplexing called Time Division Multiplexing (TDM). Bell's system is known as a T-Carrier, which can be divided into **24 64kbps sending and receiving channels**. Each channel is sampled 8,000 times per second, with each sample using 8 bits; this is known as the DS-0 rate. T1 lines can be run over copper wire.

E1

- Europe and Mexico's equivalent of a T1
- Full-Duplex
- Comprises 30 DS0 circuits bundled
- 2'048 Mbps

T3 (DS3)

- Referred to as DS3.
- Comprises 28 DS1s or 672 DS0s bundled.
- 44-736 Mbps
- Voice and Data-grade service.

OC-3

- Optical Carrier 3 uses fiber
- Is made up of 3 DS3 or 2'016 DS0s bundled.
- 155.2 Mbps

OC-12

- Optical Carrier 12
- Is made up of 4 OC-3s or 8'064 DS0s bundled.
- 622.08 Mbps

OC-48

- Optical Carrier 48 uses fiber
- Is made up of 4 OC-12s or 32'256 DS0s bundled.
- 2'488.32 Mbps

ATM

- Dial-up
- 155 Mbps to 622 Mbps
- Uses a fixed 53-byte cell to transmit data

Switched 56 Lines

- Telephone company digital dial-up service that is available upon demand. A client using a CSU/DSU can dial up another client who is using the switched 56 service. Switched 56 does not require an expensive dedicated line.

ISDN

- 2 x 64Kbps B-channels and one 16 Kbps D-channel. ISDN provides a high-speed rate called Primary Rate Interface (PRI). PRI consists of 23 B-channels and one 64-Kbps D-channel (D-channel is used for signaling and link management functions).

PSTN

- Public Switched Telephone Network
- Dia-up
- Services:
 1. Basic Voice
 2. Voice/minimum quality control
 3. Voice/radio with tone conditioning
 4. Data/below 1200 bps
 5. Basic data
 6. Voice/data over trunk circuits
 7. Voice/data over private lines
 8. Voice/data between computers over trunks
 9. Voice/video
 10. Application relays

WAN Connection Types

Dedicated (Leased Lines)

- Point-to-Point connections
- Goes from the CPE through the DCE switch, then over to the CPE of the remote site.
- Uses synchronous serial lines up to **45 Mbps**.
- **HDLC** and **PPP** encapsulation are frequently used on leased lines.

Circuit Switching

- Think phone call.
- No data can transfer before an **end-to-end connection** is established.
- Once a link is established it **remains** the same throughout the conversation.
- Circuit switching uses **dial-up modems** or **ISDN**.

Packet Switching

- Shares bandwidth with other companies to save money.
- Frame Relay and X.25 are packet-switching technologies.

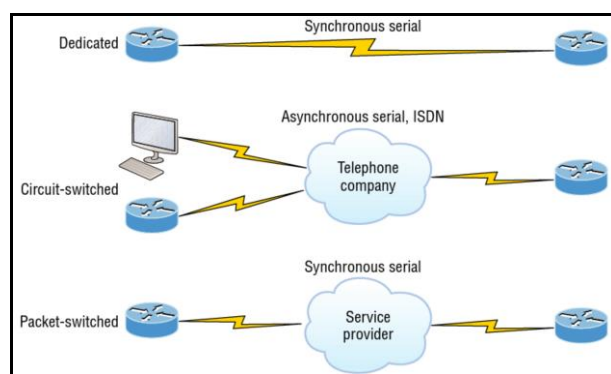


Figure 80: WAN Connection Types

MPLS uses a combination of circuit switching and packet switching technologies.

Note: You can't configure an Ethernet encapsulation on a serial interface or vice versa!

```
(config)#int s0/0/0
(config-if)#encapsulation ?
    atm-dxi
    frame-relay
    hdlc
```

lapb
ppp
smds
x25

WAN Protocols

ATM - Asynchronous Transfer Mode

- **Cell-switching** technology.
- **Connection-oriented** packet-switching technology.
- For **time-sensitive traffic**.
- Simultaneous transmission of **voice, video** and **data**.
- ATM uses cells, that are **fixed 53-bytes long** instead of packets.
- Can use either **PVCs** or **SVCs**.

Cable

- Typically, users get an access speed from **256 Kbps to 6 Mbps**.
- Cost effective connection for a small office or home office (SOHO).

Terms:

- Headend
- Distribution Network
- Data Over Cable Service Interface Specification (DOCSIS)

Cellular 3G

- Access through your phone to the @Internet.
- Get a 3G card for your ISR for backup reasons.

Cellular 4G

- Access through your phone to the @Internet.
- Get a 4G card for your ISR for backup reasons.

Cellular 5G

- Access through your phone to the @Internet.
- Get a 5G card for your ISR for backup reasons.

Cisco Intelligent WAN (IWAN)

- The Cisco IWAN enables application service-level agreements (SLAs), endpoint type, and network conditions so that **Cisco IWAN traffic** is dynamically routed to deliver the best-quality experience.
- Automate branch router configuration and management with **software-defined WAN (SD-WAN)** technology.

Cisco Long Range Ethernet (LRE)

- Employs VDSL.
- Uses twisted pair wiring.
- Speeds from 5 to 15 Mbps (full duplex).
- Distance up to 5'000 feet (1'524 m).
- Can give broadband service on POTS, digital telephone and ISDN traffic lines.

Frame Relay

- Early 1990s
- **Layer 2** WAN service

- **Nonbroadcast Multi-access (NBMA)** network.
- Packet-switched technology supported on **Serial Interfaces** and **ISDN**.
- High performance Data Link and Physical Layer specification.
- Successor of X.25
- More cost effective than Point-to-Point links.
- Speed 64 Kbps up to 45 Mbps (T3)
- Features: **Dynamic bandwidth allocation** and **congestion control**.
- Frame Relay operates using “**virtual circuits**”.
- Requires **DTE/DCE** equipment at each connection point.
- Data Terminal Equipment (**DTE**) identified by Data Link Connection Identifiers (**DLCIs**).
- **DLCIs** (Layer 2 addresses) are used by the provider to find the other end of your PVC.
- Data Communications Equipment (**DCE**)
- You can't use **HDLC** or **PPP** with Frame Relay.
- **Inverse ARP (IARP)** is mapping a DLCI to an IP Address.
- **Local Management Interface (LMI)** is a signaling standard used between your router and the first Frame relay switch it's connected to. There are 3 types (autosensed):
Cisco, ANSI and Q.933A.
Cisco default: LMI DLCI 1023
- The router exchanges **LMI information** with the Frame Relay switch **every 10 seconds**.
- **LMI** signal exchanges are also referred to as **keepalives**.
- Every **60 seconds**, routers send **Inverse ARP** messages on all active data link connection identifiers (DLCIs).
- **Point-to-Point subinterfaces** solve split horizon issues.
- If you're running Frame Relay today, you will be running **Frame Relay over Ethernet**.

Access Rate

- The maximum speed at which the Frame Relay interface can transmit.

Committed Information Rate (CIR)

- CIR is the rate, in bits per second.
- The maximum bandwidth of data guaranteed to be delivered. Everything beyond the CIR is a **burst**.
- **Bursts** can be dropped by traffic policy
- Everything beyond the CIR will be delivered as “**best effort**” and is marked as **discard eligible**.
- **MBR** is the maximum burst rate.
- If you send data six times the CIR, this is called “**oversubscription**”.

FECN, BECN, DE bits. These bits report congestion:

FECN = Forward Explicit Congestion Notification bit
BECN = Backward Explicit Congestion Notification bit
DE = Discard Eligibility bit

Frame Check Sequence (FCS) Field.

- Since one cannot completely ignore the bit error-rate of the medium, each switching node needs to implement error detection to avoid wasting bandwidth due to the transmission of *erred* frames.
- The error detection mechanism used in Frame Relay uses the cyclic redundancy check (**CRC**) as its basis.

Virtual Circuits

- There are two types of virtual circuits:
 - Permanent Virtual Circuit (**PVC**)
Like a dedicated leased line.
 - Switched Virtual Circuits (**SVC**)
Like a phone call)

Configuring Frame Relay

```
(config)#int [s0/0]
```

```
(config-if)#encapsulation frame-relay → IETF if non Cisco
```



```
(config)#int [s0/0.101] point-to-point      → Multiple PVCs, use subinterfaces.
(config-if)#encapsulation frame-relay      → IETF if non Cisco

(config-if)#ip address 172.16.20.1 255.255.255.0
(config-if)#frame-relay lmi-type [cisco | ansi | Q.933A]
(config-if)#frame-relay interface-dlci [x] → Config local DLCI

(config-if)#encapsulation ietf

frame-relay map
frame-relay map ip 172.16.100.1 100 broadcast → Broadcast = Forward packets of the
                                                PVC such as RIP updates
```

Troubleshooting Frame Relay

- **FECN** transmitted from source, is a request to slow down requests.
- If your **FECN** count is incrementing, the local PVC is congested.
- If your **in BECN** count is increasing, then the remote PVC is congested.

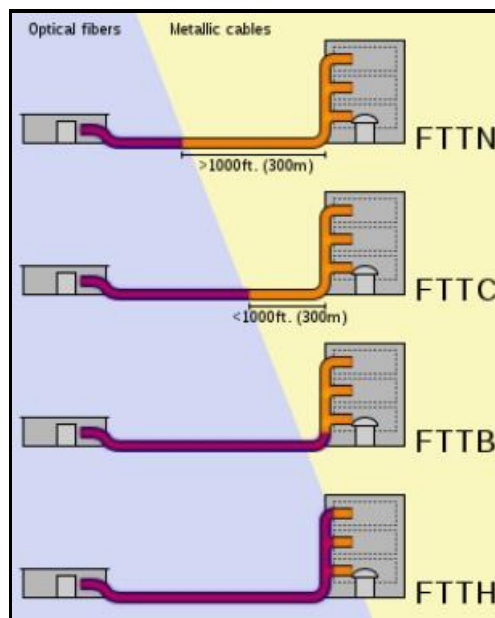
```
#show frame-relay map      → Verify DLCI destination address and encapsulation type
#show frame-relay pvc      → ACTIVE = DTE-to-DTE OK
                           INACTIVE = No connection to DTE
                           DELETED = DLCI not recognized

#show frame-relay lmi
show int [s0/0]

#debug frame lmi
```

FTTx - Fiber to the x

- Fiber to the x (FTTX) is a generic term for any broadband network architecture using optical fiber to provide all or part of the local loop used for last mile telecommunications. As fiber optic cables are able to carry much more data than copper cables, especially over long distances, copper telephone networks built in the 20th century are being replaced by fiber.



SDLC - Synchronous Data Link Control

- Operates on **Layer 2**.
- Uses **polling**.
- To provide connectivity for **mainframes** such as IBM Systems.

HDLC - High -Level Data -Link Control

- Works at the Data Link **Layer 2** and creates very little overhead.

- ISO-Standard.
- Derived from Synchronous Data Link Control (SDLC / IBM).
- Uses **polling**.
- Each vendor's HDLC is proprietary.
- Bit-Oriented, **Data Link layer** protocol.
- HDLC is a **Point-to-Point** protocol used on **leased lines**.
- **No authentication** is provided by HDLC.
- Offers **flow control** and includes **error detection** and **correction**.

HSSI - High Speed Serial Interface

- Operates on **Layer 1**.
- **DTE/DCE** interface standard.
- Defines the **electrical** and **physical characteristics** of the interfaces.

ISDN

- Integrated Services Digital Network (ISDN)
- Transmits voice and data over existing phone lines.
- Cost effective solution.
- Sometime used as backup link.

Metro Ethernet (MetroE)

- Metropolitan-area Ethernet (**MAN**)
- Providing a **Ethernet** or **fiber cable** as a connection.
- **Layer 2** WAN service
- See also **Virtual Private Wire Service (VPWS)**
- See also **Virtual Private LAN Service (VPLS)**
- Customer routers (CPEs) connect to the service as a VLAN.

MPLS

- Multiprotocol Label Switching.
- Operates between **Layer 2 and Layer 3**
- Emulates some properties of a circuit-switched network over a packet-switched network.
- Forwarding inside the MPLS network is carried out solely based on the **labels** and not on IP addresses.
- A **32-bit label** is inserted between a frame's Layer 2 and Layer 3 header. This is called a **shim header**.
- Only the edge routers perform a routing lookup.
- You can use Ethernet with MPLS to connect a WAN, Ethernet over MPLS (EoMPLS)

MPLS-based VPNs can be grouped:

- Layer 2 MPLS VPNs
- Layer 3 MPLS VPNs

Layer 2 MPLS VPN

- Every router in a shared segment established **EIGRP neighborhood** with all other routers.
- All WAN interface in a multipoint topology belong to **one broadcast domain** and one **IP subnet**.
- Layer 2 MPLS VPN may be **point-to-point** or **multipoint-to-multipoint**.
- From an **OSPF** perspective, the layer 2 MPLS VPN backbone is **invisible**.

Layer 3 MPLS VPN

- In Layer 3 MPLS VPNs the **customer router (CE)** will peer with the **provider edge router (PE)**.

P2P - Peer-to-Peer

- There is also a concept called **Pay-to-Play**.
- No need of a **central server**.
- Peers are **equally privileged**, equipotent participants in the application.

Examples of P2P Networks:

- Kazaa, Limewire, BearShare, Morpheus and Acquisition.

PPP - Point-to-Point Protocol

RFC 1661

- **Layer 2** - Data Link layer protocol.
- Replaced **SLIP**.
- PPP protocol stack is specified at the **Physical** and **Data Link layers**.
- Can be used to create **point-to-point** links between different vendor's equipment.
- **Network Control Protocol (NCP)** enables **network layer** protocols to be used on a PPP connection.
- **Network Control Protocol (NCP) field** in the Data Link header is used to identify the **network Layer protocol**.
- Allows **authentication** and multilink connections over asynchronous and synchronous links.
- It relies on **Link Control Protocol (LCP)** to build and maintain data-link connections.
- The basic purpose of PPP is to transport **Layer 3** packets across a Data Link layer PPP link.
- Supports two authentication protocols: **PAP** and **CHAP** (see RFC 1334).

Three-Way Link Establishment

1. **Link** establishment phase (LCP)
2. **Authentication** Phase (optional: CHAP or PAP)
3. **Network** layer protocol phase (NCP)

Link Control Protocol (LCP)

- **Authentication** with PAP or CHAP.
- **Compression**
- **Error Detection**
- **Multilink**
- **PPP Callback**

PAP - Password Authentication Protocol

- Requires a **username** and **password only**.
- Passwords are sent in **clear text**.
- PAP is performed only upon the **initial link establishment**.
- PAP uses a **two-way handshake**.
- PAP is **not a secure** authentication protocol.
- PAP may be vulnerable to **playback** and **trial-and-error attacks**.
- Supports **bi-directional (two-way)** and **unidirectional (one-way)** authentication.

CHAP - Challenge Handshake Authentication Protocol

- Uses a **three-way handshake**.
- Provides a **challenge** to the client.
- Generates a **unique string** for each transaction.
- **Periodical Authentication** after link establishment.
- Requires a **username** and **optional password**.
- CHAP is **more secure** than PAP.

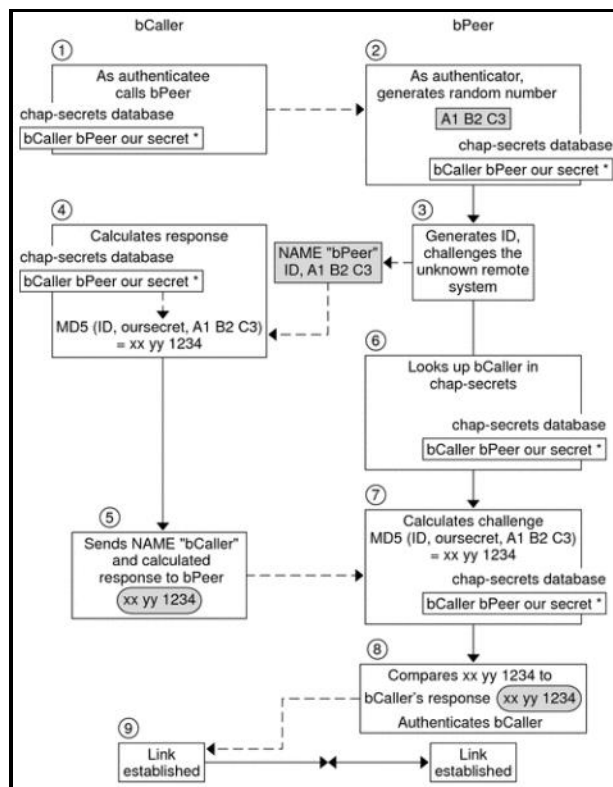


Figure 81: CHAP authentication sequence

Configuring PPP

```
(config-if) #encapsulation ppp
(config) #hostname RouterA
(config) #username RouterB password [cisco]
(config) #ppp authentication chap pap
```

For one-way authentications

```
(config-if) #ppp authentication chap callin
```

For two-way authentications

```
(config-if) #ppp authentication chap
```

Troubleshooting PPP

Note: Routers by default, use their hostname as the username when sending packets for PPP authentication.

Negotiation and authentication steps:

- DOWN
- ESTABLISHING
- AUTHENTICATING
- UP
- TERMINATING

```
#show int [s0/0]
#show cdp neighbors detail
```

```
#debug ppp authentication
#debug ppp negotiation
```

SMDS - Switched Multimegabit Data Service

- **Connectionless** packet-switching technology.
- Often used to form a **Metropolitan Area Network (MAN)**.
- Forerunner of **ATM**.

L2F - Layer 2 Forwarding Protocol

- Cisco proprietary.
- Does not offer *encryption*.

L2TP - Layer 2 Tunneling Protocol

- Supports *TACACS+* and *RADIUS*.
- Is not compatible with *NAT*.
- Works on *Layer 2*, Data Link Layer.

PPTP - Point-to-Point Tunneling Protocol

RFC 2637

- Works on *Layer 2* (encryption)
- Creates a *Point-to-Point tunnel* between two systems and *encapsulates PPP packets*.
- Authentication by: MS-CHAP, CHAP, PAP, EAP and SPAP.
- PPTP does not support *TACACS+* and *RADIUS*.
-

PPPoE - PPP over Ethernet

Authentication: *CHAP* can be used.

- Point-to-Point over Ethernet encapsulates *PPP frames* in *Ethernet frames*.
- Functions as *Layer 2* encapsulation method.
- Usually in conjunction with *xDSL services*.
- It has a *lower maximum transmission unit (MTU)* than standard Ethernet has.
- Main feature, it adds a direct connection to *Ethernet* interfaces while also providing DSL support.
- Is initiated by the *client*.
- *IPv6* is supported
- *ATM PVC* supports PPPoE client.

Configuring PPPoE Client

1. Create a *dialer interface* using the `interface dialer [number]` command.
2. Instruct the client to use an IP address provided by the PPPoE server with the `ip address negotiated` command
3. Set the encapsulation type to PPP.
4. Configure the dialer pool and number.
5. Under the physical interface, use the `pppoe-client dial-pool-number [number]` command

```
(config)#interface dialer 1
(config-if)#ip address negotiated          → Dynamically acquire an IP address
(config-if)#encapsulation ppp
(config-if)#dialer pool 1
(config-if)#mtu 1492
(config-if)#interface [f0/1]
(config-if)#no ip address
(config-if)#pppoe-client dial-pool-number [1]
(config-if)#pppoe-client ppp-max-payload 1500
=====
(config)#vpdn enable                      → Enables VPDN on the router
dialer persistent                         → Dial-on demand routing to be permanent enabled
```

Troubleshooting PPPoE Client

```
#show ip int brief
#show pppoe session

#debug ppp negotiation
```

PPP over ATM (PPPoA)

RAN - Radio Access Network

- A **radio access network (RAN)** is part of a mobile telecommunication system. It implements a radio access technology. Conceptually, it resides between a device such as a mobile phone, a computer, or any remotely controlled machine and provides connection with its core network (CN). Depending on the standard, mobile phones and other wireless connected devices are varyingly known as user equipment (UE), terminal equipment, mobile station (MS), etc.
- RAN functionality is typically provided by a silicon chip residing in both the core network as well as the user equipment. See the following diagram:

VSAT

- Very Small Aperture Terminal
- For many locations geographically spread out in a large area.
- Two-way satellite ground station with dishes available through many companies like Dish Networks or Hughes.

xDSL

- Digital Subscriber Line.
- DSL connections are deployed in the last mile of a local telephone network - the local loop,
- Uses copper phone wires.
- ADSL, HDSL, RADSL, SDSL, IDSL and VDSL.
- SDSL and IDSL can carry only data.
- Up to 6.1 Mbps

Symmetrical DSL (SDSL)

- Speed of downstream and upstream are equal.
- SDSL has a service distance of 12'000 feet (3'658 m) at high speed.

Asymmetrical DSL (ADSL)

See: Asymmetric Digital Subscriber Line

Is a type of digital subscriber line (DSL) technology, a data communications technology that enables faster data transmission over copper telephone lines than a conventional voice band modem can provide. It does this by utilizing frequencies that are not used by a voice telephone call. A splitter, or DSL filter, allows a single telephone connection to be used for both ADSL service and voice calls at the same time. ADSL can generally only be distributed over short distances from the telephone exchange (the last mile), typically less than 4 kilometers (2 mi), but has been known to exceed 8 kilometers (5 mi) if the originally laid wire gauge allows for further distribution.

Source: Wikipedia

- Different transmission speeds downstream and upstream.
- Downstream speed is always faster.
- ADSL has a service distance of 18'000 feet (5'486 m).
- Supports both voice and data.
- Downstream rate from 256 Kbps to 8 Mbps.
- Upstream up to 1.5 Mbps max.
- ATM is the Data Link layer protocol typically used over the DSL layer 1 connection from the CPE and is terminated at what's known as the **DSLAM**.

Route Redistribution

- Used for instance if companies are **merging** and using different protocols (OSPF/EIGRP).
- Redistribution uses the one table that the routing protocols understand, the **IP routing table** a route must be in the routing table to be advertised.
- The redistributed routes are treated as **external routes**
- Redistribution design calls for a **minimum of two routers** performing redistribution.

- **EIGRP** does not have a default setting for the metric when trying to redistribute **OSPF into EIGRP**
- The router performing redistribution into **OSPF** becomes an **ASBR**
- **OSPF** creates **LSAs** to represent each external route
- **OSPF E1 routes** are based on **internal cost plus external cost**. Use the redistribute command with parameter `metric-type 1`
- **OSPF E2 routes** are working well based only on the **external metric**. Use the redistribute command with parameter `metric-type 2`
- **OSPF** always prefers **E1** route over an **E2** route
- Only **OSPF** routers in **NSSAs** can redistribute routes with **Type-7 LSAs**.
- The **default external metric type** for routes redistributed into **OSPF** is **Type-2** with a **default metric of 20**.
- **BGP routes** redistributed into OSPF have a **default metric of 1**.

Methods of setting Metric for Redistribution into EIGRP:

1. `default-metric [bw delay reliability load mtu]`
The **default-metric** values are only used if a redistribute command does not include those values using the **metric option**.
If the **metric option** is used, the **default-metric** command is ignored.
2. `redistribute [ospf] [2] metric [bw delay reliability load mtu]`
3. `route-map`

One-Way Redistribution:

- **One-Way** redistribution at one point is always safe to perform.
- Represents the only exit and the only entrance from one routing protocol to another.
- **Multipoint One-Way** redistribution may result in **routing loops**.
- **Multipoint One-Way** works only well if the receiving protocol supports different administrative distances for internal and external routes. This are EIGRP, BGP and OSPF.

Two-Way Redistribution:

- **Two-Way** redistribution is always safe because two-point redistribution represents the only exit and the only entrance from one routing protocol to another.
- **Multipoint Two-Way** redistribution only considers part of the cost in making routing decisions.
- **Multipoint Two-Way** redistribution may result in **routing loops** and **suboptimal routing**.
To avoid routing loops:
 - **Tag** routes in redistribution points and filter based on tags when doing redistribution.
 - Insert **only internal routes** from routing protocol A to B and vice versa.
 - Use **default routes** to avoid two-way redistribution.
- **Multipoint Two-Way** redistribution loses the metrics.

Route-Map:

- A **route-map** performs **matching, modification** and **filtering** based on **several types of matches**, and it uses **ACLs** if the required matching is to be based on addressing information.
- Identify the subsets of the routes to **filter or change** based on the route's prefix/length, plus many other factors.
- Make filtering choices about **which routes are redistributed and which are not**.
- Set the metric to different values based on information matchable by the route-map.
- Set the type of external route for different redistributed routes, for example, OSPF **Type-1** for some routes and **Type-2** for others.
- Set a **route tag**, a unit less integer value that can later be matched with a route-map at another redistribution point.
- For **OSPF** use the redistribute **match and set option** to filter routes.
- If there is no match in a route-map sequence **Automatic Matching** occurs.
- If IOS matches a route-map permit clause, and the set command includes the default parameter, the IOS will attempt **to route the packet normally ignoring any default routes**.
- If IOS matches a route-map permit clause, and the set command includes the default parameter and there isn't a match with a nondefault route, then **the router forwards the packet using the set command**.
- Match criteria in the same line of a route-map are processed with **OR** logic.
- Match criteria **vertically** aligned in a route-map, uses **AND** logic.
- Route-map are preventing **routing loops** by using **Route-Tagging** and Redistribution of **internal routes**.
- Route-Maps can be used to **load balance** traffic between ISPs.

- Is used to **filter routing updates**.

```
ip access-list extended match-101
permit ip host 172.16.101.0 host 255.255.255.0
ip prefix-list match-101
route-map option1 deny 10
match ip address match-101
```

```
-----
route-map set metric permit 10
match ip address prefix-list match-102-103
set metric 1000 44 255 1 1500
-----
```

MATCH Command

```
match interface [x]
match ip address [x]
match ip next-hop [ACL]
match ip route-source [ACL]
match metric [x]
match route-type [x]
match tag [x]
```

SET Command

```
set metric [x]
set metric [bw delay reliability loading mtu]
set metric-type [type-1 | type-2]
set tag [x]
```

BGP path selection

```
(config)#route-map MY-ROUTE-MAP permit 10
match local-preference 150
set weight 200
neighbor 10.0.0.1 route-map MY-ROUTE-MAP in
```

Set a Tag

```
set tag [nr.]
```

Prefix-List:

- **Replaces ACLs** to filter routing updates.
- Is used to **filter routing updates**.

```
ip prefix-list OSPF_REDIST seq 5 deny 10.0.0.0/24
ip prefix-list OSPF_REDIST seq 5 permit 0.0.0.0/0 le 32
route-map OSPF->BGP permit 10
match ip address prefix-list OSPF_REDIST
```

Distribute-List:

- A distribution list is really only a command that **uses route-maps, numbered ACLs, named ACLs** or **prefix-lists** to perform filtering of routing information advertised or received within a particular routing protocol.
- It's **not a standalone filtering mechanism** like ACLs/route-map.
- It's used to control **Routing Updates** no matter what their source is.

Route tag:

- A route tag is a unit less 32-bit integer that most routing protocols can assign to any given route.

Configuring Redistribution

```
-----
(config)#router eigrp [1]
(config-router)#redistribute ospf [2]
(config-router)#default-metric x x x x x
```

```
-----
(config)#router ospf 2
```



```
(config-router)#redistribute eigrp [1]
-----
(config)#router rip
(config-router)#redistribute ospf [PID] metric 3
-----
(config-router)#redistribute eigrp [1] subnets
(config-router)#redistribute eigrp [1] subnets metric-type 1    → Creates E1 route
(config-router)#redistribute eigrp [1] subnets metric-type 2    → Creates E2 route
```

Troubleshooting Redistribution

```
#show ip route [IP] [SN] longer-prefixes
```

Route Selection

- **Cisco Express Forwarding (CEF)** is a feature that allows a router to very quickly and efficiently make a route lookup. Predecessors are **Process Switching** and **Fast Switching**.
- **Policy-Based Routing (PBR)** also called **Policy Routing** influences the IP data plane, changing the forwarding decision a router makes, but without first changing the IP routing table.

Policy-Based Routing (PBR)

- PBR chooses how to forward the packet by using **matching logic** defined through a **route-map**, which in turn typically refers to an IP **access control list (ACL)**.
- Omitting the `default` parameter gives you the following logic: **"Try PBR first, and if PBR's route does not work, try to route as usual."**
- Including the `default` parameter gives you logic like this: **"Try to route as usual while ignoring any default routes, but if normal routing fails, use PBR."**
- PBR supports **Class-Based Marking (QoS)**.

Configuring PBR

- Create a route-map with the logic to match packets.
- Enable the route-map for use with PBR.

```
(config-if)#ip policy route-map [name]
(config-if)#route-map [name]
(config-if)#match ip address [101]
(config-if)#set ip next-hop [next hop]
(config-if)#access-list [101] permit ip host [source] [destination] [wc]
```

```
ip local policy route-map [name]    → For packets created on the router
set ip precedence [value]
set ip tos [value]
set interface                        → Use the first interface in the list
```

Troubleshooting PBR

```
#show ip policy                      → Verifying the configured policies
show route-map
```

```
debug ip policy
```

```
traceroute
```

Virtual private dial-up networks (VPDNs)

- VPDNs securely **carry private data over a public network**, allowing remote users to access a private network over a shared infrastructure such as the Internet.
- VPDNs maintain the same security and management policies as a private network, while providing a cost-effective method for **point-to-point** connections between remote users and a central network.

Troubleshooting VPDN

```
#show vpdn
#show vpdn session
#show vpdn tunnel
```

Virtual Routing and Forwarding (VRF)

- Virtualized Networks
- VRF allows a single physical router to host **multiple virtual routers**.
- Legacy: **VRF-Light**.
- Uses a **subinterface** on each router for the VRF.
The new **Cisco Easy Virtual Network (EVN)** uses Virtual Network Trunk (VNET Trunk) instead and uses tags to identify the the virtual networks to which packets belong.

Components of a VRF:

- Subset of the router interfaces
- Associated routing protocol instances
- A routing table or RIB
- Associated forwarding data structures or FIB

Virtual routing and forwarding (VRF) is a technology included in IP (Internet Protocol) network routers that allows **multiple instances of a routing table to exist in a router and work simultaneously**. This increases functionality by allowing network paths to be segmented without using multiple devices. Because traffic is automatically segregated, VRF also increases network security and can eliminate the need for encryption and authentication. @Internet service providers (ISPs) often take advantage of VRF to create separate virtual private networks (VPNs) for customers; thus, the technology is also referred to as VPN routing and forwarding.

VRF acts like a **logical router**, but while a logical router may include many routing tables, a VRF instance uses only a single routing table. In addition, VRF requires a forwarding table that designates the next hop for each data packet, a list of devices that may be called upon to forward the packet, and a set of rules and routing protocols that govern how the packet is forwarded. These tables prevent traffic from being forwarded outside a specific VRF path and also keep out traffic that should remain outside the VRF path.

Source: Wikipedia

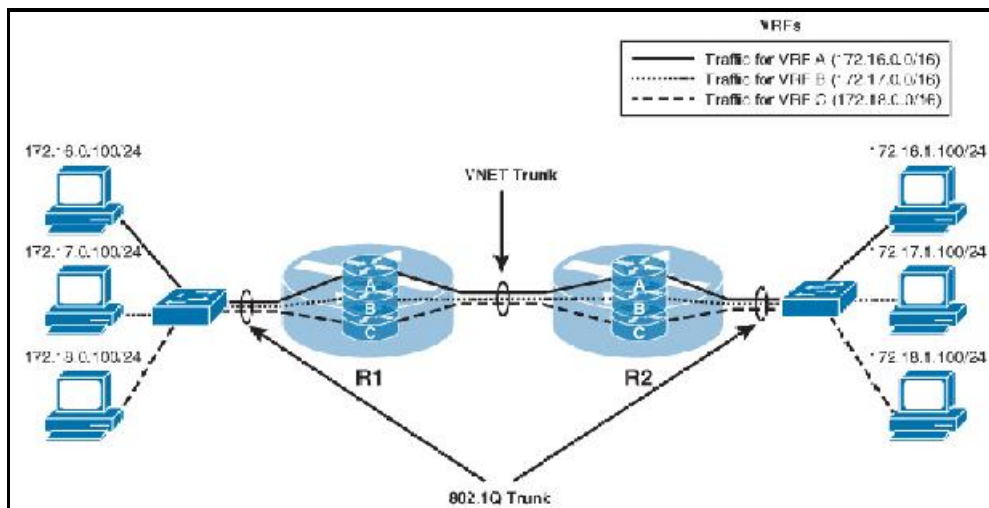


Figure 82: Sample EVN Topology

Pros:

- Increases **network security** and can eliminate the need for **encryption** and **authentication**.
- Meets, **Sarbanes-Oxley Act** and the **HIPAA Privacy Rule**.

Cons:

Configuring VRF:

```
ip routing →
ip vrf [x] →
rd [route distinguisher] →
route-target [export|import|both] → Only if BGP is running!
import map [route-map] →
interface [IF] →
ip vrf forwarding [x] →
```

```
(config)#ip route vrf → Establish static routes
```

Troubleshooting VRF:

```
#show ip vrf
#show ip vrf brief
#show ip vrf detail
#show ip route vrf [name]

#ping vrf [VOICE] 10.1.1.1
```

VRF-Lite

- **Legacy** but still often used.
- VPN routing and forwarding customer edge (**VRF CE**) feature is also called VRF-Lite.
- With VRF-Lite, a router is configured with **multiple subinterfaces**, one for each VRF.

Configuring VRF-Lite:

```
ip vrf [name]
ip vrf forwarding [name]
router ospf [process-id] vrf [name]
```

Multi-VRF

- Using Multi-VRF CE, you can configure more than one instance of a routing and forwarding table within a single customer edge (CE) router.
- To use OSPF as the routing protocol between the provider edge (PE) and the CE, you need to issue the `capability vrf-lite` subcommand under the OSPF routing process.

Configuring Multi-VRF:

```
capability vrf-lite
```

Next Hop Resolution Protocol (NHRP)

- In a computer network, the Next Hop Resolution Protocol (NHRP) is a protocol or method that can be used so that a computer sending data to another computer can learn the **most direct route** (the fewest number of hops) to the receiving computer.
- If the receiving computer is in the **same subnetwork**, the use of NHRP will tell the sending computer that the receiving computer is local and it can send subsequent data packets directly to the receiving computer **using its subnetwork address** rather than its global network address.
- If the receiving computer is **not in the same subnetwork**, the use of NHRP will tell the sending computer the computer in the subnetwork **whose router provides the most direct path** to the receiving computer and the sender can now forward subsequent data packets to that router.
- It plays a role in Cisco's **DMVPN**, to map physical IP addresses to logical IP addresses.
- NHRP is an ARP-like protocol that allows **Next Hop Clients (NHCs)** to dynamically register with **Next Hop Servers (NHSs)**.
- NHRP is using the **Client/Server** model.
- **Hub & Spoke** concept, the **spoke routers** are configured with the IP address of the **hub router**.

- NHRP does not support the aggregation of nonbroadcast multiaccess (NBMA) information thus the IP-address has always a **netmask of /32**.

Flags:

- **authoritative** = NHRP information obtained from the next-hop server (NHS)

Process:

1. NHRP sends a query to the hub router asking what physical IF IP-address is associated with a tunnel.
2. The hub router checks its NHRP database and responds to the query with the IP-address.
3. The router builds the dynamically learned tunnel.

Configuring NHRP

```
interface type number
ip address ip-address network-mask
ip nhrp network-id number
```

REDIRECT & SHORTCUT

- Used in DMVPN Phase III.
- Works like a ICMP redirect.

```
(config-if) #ip nhrp shortcut
(config-if) #ip nhrp redirect
```

Troubleshooting NHRP

```
#show ip nhrp → Shows tunnel name and Flag
#show ip nhrp detail
```

Apple Networks

AppleTalk

- Macintosh computers have built-in AppleTalk networking capabilities.
- AppleTalk Phase II is the latest Version of AppleTalk from Macintosh.
- AppleTalk UTP networks uses **Bus Topology with STP cabling**
- **And Tree Topology with UTP**. AppleTalk uses the Macintosh cabling specifications known as LocalTalk.

LocalTalk

- The LocalTalk specification is a **CSMA/CA access method in a bus or tree Topology**.
- LocalTalk is usually run over **STP**, but it can **also use fiber-optic and UTP**.
- LocalTalk networks **only support 32 devices**.
- They are often **Replaced** by third-party solutions such as **Farallon PhoneNet**, which can support **up to 254 devices**.

AppleShare

- AppleShare is the Macintosh file server software included with every Apple Computer.
- LocalTalk networks are divided into zones, which can be interconnected to form larger networks.

EtherTalk

- EtherTalk is the Macintosh equivalent of Ethernet.
- It is used for running AppleTalk **over thinnet and thicknet** Networks.
- Compatible with AppleTalk Phase II.

TokenTalk

TokenTalk is the Macintosh equivalent of Token Ring. It is used for running AppleTalk over Token Ring Networks with the **802.5 specification**. Compatible with AppleTalk Phase II.

CABLING

- HDLC, PPP and Frame Relay can use the same Physical Layer specification.

Serial Transmission

- 1 bit at a time over a single channel.
- Cisco's old 60-pin serial connector.
- The new Smart-Serial connector.
- EIA/TIA-232
- EIA/TIA-449
- V.35
- EIA-530

DTE-DCE-DTE WAN Connection

- By default, router interfaces are typically DTEs, and they connect into DCE like a CSU/DSU using a V.35 connector.
- The idea behind a WAN is to be able to connect two DTE networks through a DCE network.
- CSU/DSU provides clocking.

#show controllers [s0/0/0]

→ Clock rate 2000000 default for ISR

SDN - Software Defined Networking

RFC 6244

- Should be called **SDx** today.
- Needs "**Hybrid Engineers**".
- **SDN** decouples network management to modify networking devices directly.
- It set an abstract layer (Control Plane) above and the management is more on the logical level.
- The logical level will be applied to the different involved devices (Data Plane).
- **Programmatic control** of network infrastructure.
- Target is to reduce cost of **CAPEX** and **OPEX**.
- Helps moving away from **CLI**.
- See the **Open Networking Foundation (ONF)**

Segregation of:

- Control Plane
- Data Plane

Programmatic Interfaces:

- RESTconf
- NETCONF
- gRPC
- YANG
- Python
- Postman

APIs

- Cloud-Level APIs
- Controller-Level APIs
- Infrastructure-Level APIs

Check out Cisco's "**DevNet**"

<https://learninglabs.cisco.com/labs/tags/Coding>

YANG

RFC 6020, 6021, 7950

- **Modeling language.**
See: <https://github.com/YangModels/yang>
- Represents **configuration, operational state, transactions** and **notifications**.

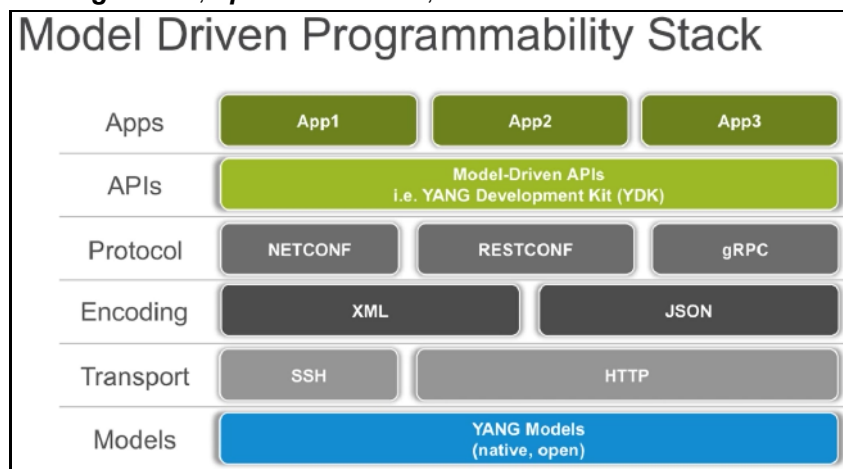


Figure 83: Programmability Stack

Data structured as a tree:

- Leaf
- Leaf List

- Container
- List

Tools:

- PYANG <https://github.com/mbj4668/pyang>
- YANG Development Kit <https://developer.cisco.com/site/ydk>

REST

- Links: <https://learninglabs.cisco.com>
<https://github.com/CiscoDevNet>
<http://www.pyhton.org>
<http://www.getpostman.com>
<http://www.git-scm.com>

Authentication:

- Basic HTTP
- OAuth
- Token

Cisco APIC-EM

- Cisco **Application Policy Infrastructure Controller - Enterprise Module (APIC-EM)** is a **Cisco SDN controller** which uses API's for policy-based management and security through a single controller, abstracting the network and making network services simpler.
- It uses a service abstraction layer (**SAL**) which talks to the network elements via **SNMP** and **CLI**.
- The **API** is **REST** based, which allows you to discover and control your network using **HTTP** with GET, POST, PUT and DELETE options along with **JSON** and **XML**.

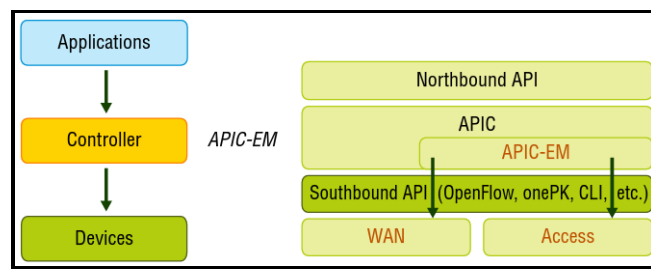


Figure 84: Where APIC EM fits in the SDN stack

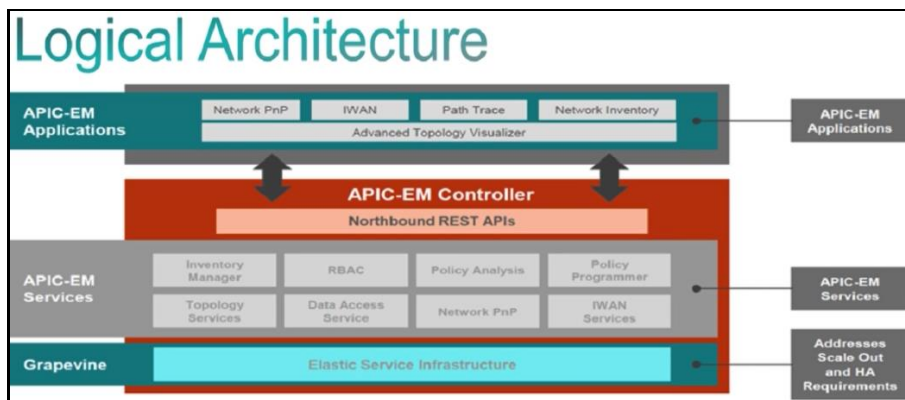


Figure 85: Logical Architecture

Functions:

- Discovery
- Device Inventory
- Host Inventory
- Topology
- IWAN

- Path Trace
 - Filters
- Network Plug & Play

Pros:

- Single point of control of the network
- Deploy network devices faster
- Increase productivity
- Provide programmable network
- Offer a great application experience
- Reduces cost (OPEX)

Southbound API (Cisco ACI)

- **OpFlex**, an open-standard distribution control system.

Path Trace App

- Discovers and visualizes path between two end points.
- Needs 5-tuple input:
Source, Source-Port, Protocol, Destination, Destination-Port.

Quality of Service (QoS)

- QoS is the measure of **transmission quality** and **service availability** of a network (or internetworks).
- It's basically the ability to provide a different priority to one or more types of traffic over the levels of different applications, data flows, or users so that they can guaranteed a certain performance level.
- IP header's type of service (**ToS**) byte is used.
- See also **3-bit IP precedence (IPP)** field and **Differentiated Services (DS) byte** and the **Differentiated Service Code Point (DSCP)**.
- The target for **High Availability is 99.999 % uptime**, with only five minutes of downtime permitted per year.

QoS focus:

- Delay
- Dropped Packets
- Error
- **Jitter**

Not every packet takes the same route to the destination, so some will be more delayed than others if they travel through a slower or busier network connection. The variation in packet delay is called jitter.

- Out-of-Order Delivery

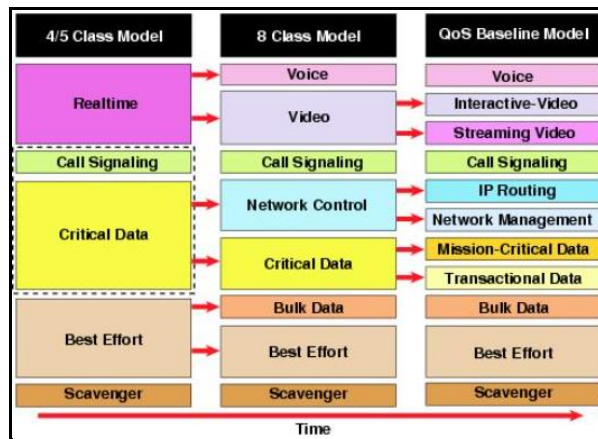


Figure 86: QoS Strategy

HCI - Hyperconverged Infrastructure

- Hyperconverged infrastructure (HCI) combines **compute**, **virtualization**, **storage**, and **networking** in a single cluster.
- Starting with as few as **three nodes**, users can easily scale out to match computing and storage resource needs.
- Hyperconvergence brings **cloudlike simplicity on-premises** and within a single, easily managed platform.
-

SDN Solutions

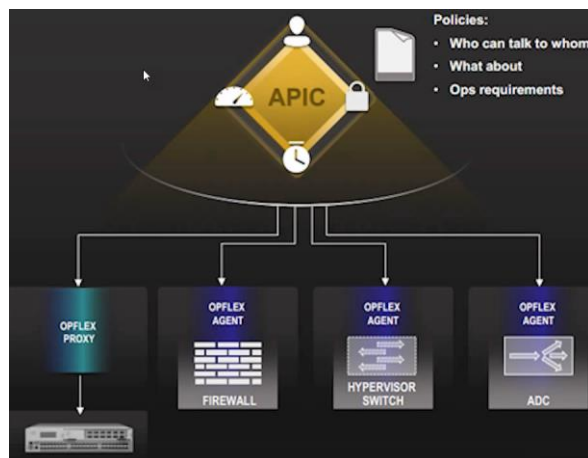
- Solarwinds - Network Performance Monitor (NPM).

OpenDaylight

- Source: <https://www.opendaylight.org/>
- OpenDaylight, is an open source SDN controller.
- Developed in Java and used also by Cisco.

OpFlex

- Is a open standardized **API** with an open source reference implementation.
- **Abstract policies** rather than device-specific configuration.
- Opflex uses **declarative policies**.
- Flexible, extensible definition of using **XML/JSON**.
- Cisco OpFlex is a **southbound protocol** in a software-defined network (**SDN**) designed to facilitate the communications between the SDN Controller and the infrastructure (switches and routers).
- The goal is to create a **standard** that enables policies to be applied across physical and virtual switches/routers in a **multi-vendor environment**.



OpenFlow

- Was designed to facilitate **separation of control** and **data planes** in a standardized way.
- To control the **forwarding plane**.

UCS - Cisco Unified Computing System

<https://developer.cisco.com/site/ucs-dev-center>

- UCS Manager
- See also **SDN**
- Makes use of the **XML API**
- Communication over **HTTP/HTTPS**
- Use the **UCS emulator** (UCSPE).



Figure 87: Cisco Unified Computing System

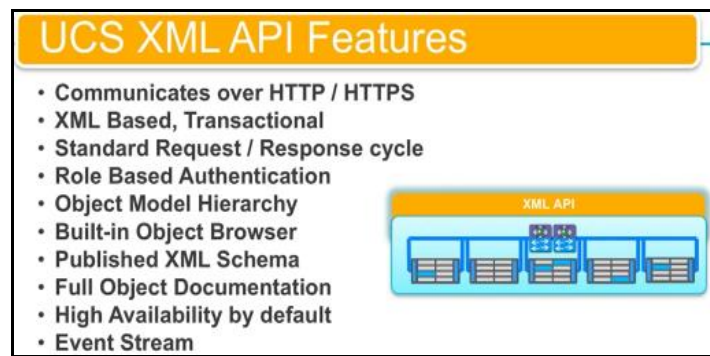


Figure 88: UCS XML API Features

I2RS - Interfaces to the Routing System

SDDC - Software Designed Datacenter

- Ein SDDC (Software-defined Data Center) ist eine Infrastruktur, in der alle Elemente virtualisiert sind und als Service ausgeliefert werden.
- Das gilt für Netzwerk, Storage, CPU und Security. Verwendung, Provisioning, Konfiguration und Betrieb sind komplett von der Hardware abstrahiert und werden durch Software realisiert.
- Virtualisierung ist für ein Software-defined Data Center von zentraler Bedeutung. Die drei hauptsächlichen Bausteine eines SDDC sind:
 - Netzwerk-Virtualisierung
 - Storage-Virtualisierung
 - Server-Virtualisierung.

@INTERNET CONNECTIVITY

Static IP Address Assignment

1. Assign an IP address to the router interface connecting to the ISP
`ip address [ip] [subnet-mask]`
2. Configure a default route pointing to the ISP
`ip route 0.0.0.0 0.0.0.0 [next-hop ip of ISP]`
Note: Defining the next hop is best practice.

Dynamic IP Address Assignment

1. Only one command is necessary.
`(config-if)#ip address dhcp`
`no ip dhcp client request router` → Prevents the assignment of a static route.

IPv6 INTERNET CONNECTIVITY

- When an enterprise has more than one connection to the @Internet, the use of default static routes might not be sufficient.
- MGP-4 (MP-BGP) allows the advertisement of both IPv4 and IPv6 networks.
- IPv6 comes with new security concerns.

Methods of Assigning an IPv6 Address

Method	Dynamic or Static	Prefix and Length Learned from...	Host Learned from...	Default Router Learned from...	DNS Addresses Learned from...
Stateful DHCP	Dynamic	DHCP Server	DHCP Server	Router, using NDP	(Stateful) DHCP Server
Stateless Autoconfig	Dynamic	Router, using NDP	Derived from MAC	Router, using NDP	Stateless DHCP
Static Configuration	Static	Local config	Local config	Router, using NDP	Stateless DHCP
Static Config with EUI-64	Static	Local config	Derived from MAC	Router, using NDP	Stateless DHCP

Figure 89: IPv6 Address Assignment for Global Unicast Addresses

Message	RS	RA
Multicast destination	FF02::2	FF02::1
Meaning of multicast address	All routers on this link	All IPv6 nodes on this link

Figure 90: Details of the RS/RA Process

Feature	Stateful DHCP	Stateless DHCP
Remembers IPv6 address (state information) of clients that make requests	Yes	No
Assigns IPv6 address to client	Yes	No
Supplies useful information, such as DNS server IP addresses	Yes	Yes
Most useful in conjunction with stateless autoconfiguration	No	Yes

Figure 91: Comparing Stateless and Stateful DHCPv6 Services

Methods of Assigning an IPv6 Address to a CPE

Manual Configuration

```
ipv6 address [IP]
ipv6 route ::/0 [next-hop] → Creates a IPv6 default static route
```

Stateless Address Autoconfiguration (SLAAC)

Stateless DHCPv6

DHCPv6 Prefix Delegation (DHCPv6-PD)

- DHCPv6-PD is an extension to DHCPv6.
- A DHCPv6-PD client is usually a **CPE device**.
- Assigns a collection of IPv6 networks to the router and can assign those IPv6 networks to its various interfaces.

Single Session versus Dual Session

Single IPv4 BGP Session

- **Fewer neighborships** are formed.
- When sending IPv6 route information over the IPv4 BGP session, you need to create a **route-map** to modify the Next-Hop BGP attribute.

Dual IPv4/IPv6 BGP Session

- **More neighborships** must be configured.
- You do not need to configure a **route-map** to modify the Next-Hop BGP attribute.

IPv6 Access Control List

- IPv6 ACLs are always **extended** and **named**.
- The **traffic-filer** keyword is used instead of **access-group**.
- IPv6 ACLs have three implicit instructions residing at the bottom of all ACLs

To assure that Neighbor Discovery is function properly (Default)

```
permit icmp any any nd-na
permit icmp any any nd-ns
deny ipv6 any any
```

IPv6 @Internet Connection Security

- The neighbor Discovery process used by IPv6 might be leveraged by a malicious user to launch a man-in-the middle attack. Similar to a gratuitous ARP attack in an IPv4 network.
- IPv6 addresses are no longer concealed to the @Internet.
- Protect the enterprise with a **Stateful firewall**.

VPN

- VPN is solving the security issue using the **@Internet** as transport.
- Allows the creation of private networks across the **@Internet**, enabling privacy and tunneling of non-TCP/IP protocols.
- Security: You can use advanced encryption and authentication technologies like IPSec and SSL.
- In **hybrid VPNs** you must consider **decreasing the MTU size**, because of the overhead.

There are **three types of VPN**:

- Remote Access VPN
- Site-to-Site VPNs
- Extranet VPNs

There are several **tunneling protocols**:

- Layer 2 Forwarding (**L2F**)
Cisco proprietary tunneling protocol.
- Point-to-Point Tunneling Protocol (**PPTP**)
Was created by Microsoft.
- Layer 2 Tunneling Protocol (**L2TP**)
Cisco and Microsoft.
- Generic Routing Encapsulation (**GRE**)
Cisco proprietary tunneling protocol.
- **IPSec** - IP Security Protocol

MPLS

Frame Relay

Leased Line

Cable

Digital Subscriber Line (DSL)

IPSec - IP Security VPN's

See Security.docx

Troubleshooting IPSec

`#show crypto ipsec sa`

→ Shows:
inbound crypto map
remaining key lifetime
path MTU

Secure Sockets Layer (SSL) - VPN's

Transport: Uses port **443**.

- Operates on **transport layer**.

Functionalities

- **Confidentiality**
Avoids that the packets can be read during the transport in the **@Internet**
- **Authentication**
Assures, that the sender is the correct one (Peer Authentication).
- **Message integrity**
Avoids, that packets are modified during the transport through the **@Internet**.
Uses Message Authentication Code (MAC).
- **Anti-Replay**
Avoids., that packets acopied and sent from a intruder

Types

- **Intranet-VPN/ Site-to-Site-VPN**
Main-Site / Subsidiary
Router (Main Security-Gateway)
- **Extranet-VPN**
Main-Site / Partner-Site
Router (Partner Security Gateway)
- **Remote-Access-VPN**
Main-Site / Home User
ASA (CVPN-Box)

Cisco-Adaptive Security Appliance (ASA)

S-HTTP - Secure Hypertext Transfer Protocol

RFC 2660

- Operates on the **application layer**.
- An obsolete alternative to the **HTTPS protocol**.
- Sends **individual messages** securely.
- Provides **protection for each message** sent between two computers, but not the actual link.

GRE - Generic Routing Encapsulatio (GRE Tunnel)

RFC 2784

Transport: IP protocol number **47**.

- **Generic Routing Encapsulation (GRE)** is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an @Internet Protocol internetwork.
- GRE is a tunneling protocol that can encapsulate many protocols inside **IP tunnels**. Some examples would be **routing protocols** such as **EIGRP** and **OSPF**.
- GRE can encapsulate any **Layer 3** protocol.
- GRE does not provide **encryption** or **authentication service**.
- GRE supports **broadcast** and **multicast** traffic.
- GRE supports **point-to-point** and **multipoint** links.
- GRE **bridges** the gap between two routers.
- Does not include any **flow-control** mechanisms.
- It's **stateless**.
- Recommended **MTU** size is **1400** to avoid fragmentation.

Reasons to tunnel traffic using GRE:

- You need to encrypt multicast traffic. GRE tunnels can carry multicast packets—just like real network interfaces—as opposed to using IPSec by itself, which can't encrypt multicast traffic. Some examples of multicast traffic are OSPF, EIGRP, and RIPV2. Also, a number of video, VoIP, and streaming music applications use multicast.
- You have a protocol that isn't routable, such as NetBIOS or non-IP traffic over an IP network. For example, you could use GRE to tunnel IPX or AppleTalk through an IP network.
- You need to connect two similar networks connected by a different network with different IP addressing.

Source: Wikipedia

GRE-Tunnel Interface.

- Forms **virtual point-to-point links**.
- GRE uses a **protocol-type field** in the GRE header so **any layer 3** protocol can be used through the tunnel.
- GRE is **stateless** and has **no flow control**.
- GRE has no built-in **security mechanisms**.
- GRE creates additional overhead for tunneled packets. At least **24 bytes**.

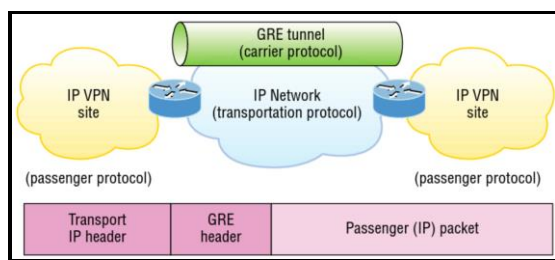


Figure 92: GRE Tunnel

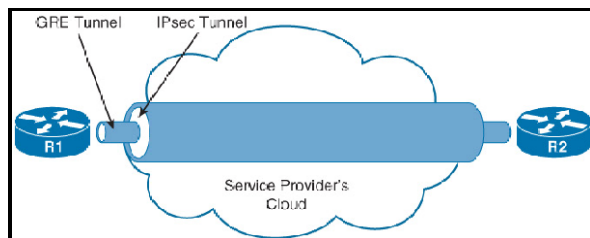


Figure 93: GRE over IPsec Tunnel

Configuring GRE Tunnels

1. Create a virtual tunnel interface.
2. Add an IP address for the virtual tunnel.
3. Specify the source of the tunnel.
4. Specify the destination of the tunnel.

```
(config)#int [s0/0]
(config-if)#ip address 63.1.1.1 255.255.255.252

(config)#interface tunnel [0]
(config-if)#tunnel mode gre ip

(config-if)#ip address 192.168.10.1 255.255.255.0
(config-if)#tunnel source 63.1.1.1
(config-if)#tunnel destination 63.1.1.2
```

Troubleshooting GRE Tunnels

- Is the physical interface flapping?
- Are the routing protocols flapping?
- Is recursive routing built in (may lead to flapping)?

```
#show interfaces tunnel [x]
#show ip interface brief
#show interfaces tunnel [0]
#show ip route
(config)#show run interface tunnel 0
```

Multipoint GRE (mGRE)

- Supports a wide variety of protocols such as **IP unicast**, **multicast** and **broadcast**.
- A single **mGRE** interface can service multiple tunnels
- Allows a router to support **multiple GRE tunnels** on a single **GRE interface**.
- mGRE uses **NHRP** to form dynamically a tunnel.

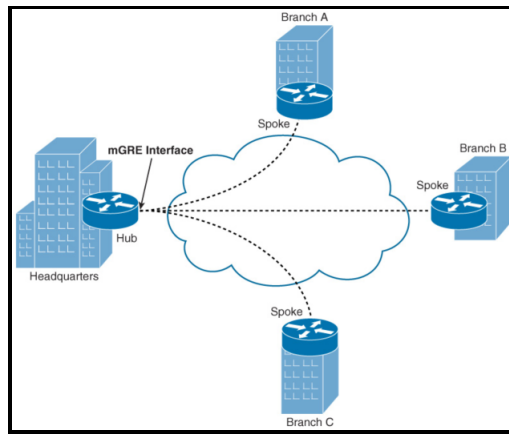


Figure 94: Hub-and-Spoke mGRE tunnel topology

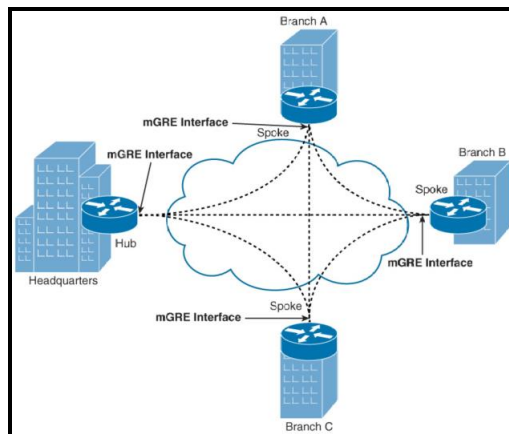


Figure 95: Spoke-to-Spoke mGRE tunnel topology

Cisco Dynamic Multipoint VPN (DMVPN)

- **Cisco Proprietary**
- **Security** in a DMVPN is provided by **IPSec**.
- Allows to easily scale large and small **IPsec** VPNs.
- Allows **low cost connection** to branch offices.
- Typical topology **hub-and-spoke** but **spoke-to-spoke** design is also supported.
- DMVPN has one central router, the **hub**.
- Branch routers are called **spoke**.
- The DMVPN feature enables you to configure a **single GRE tunnel** interface and a **single IPsec profile** on the hub router to manage all spoke routers.
- **Dynamic VPN** tunnel creation is also supported.
- Uses **mGRE** with **NHRP** to dynamically form GRE tunnels.
- A common issue with DMVPN tunnels is **flapping**.
- DMVPN can be configured in three different modes, each called a "**phase**".

DMVPN Phase I (Spoke-to-Hub only)

DMVPN Phase II (Spoke-to-Spoke)

DMVPN Phase III (Spoke-to-Spoke)

- Same as Phase II but removes some restrictions and complexities of Phase II.

Configuring DMVPN

Sync-up the timestamps between the hub and spoke

```
Enable msec debug and log timestamps
(config)#service timestamps debug datetime msec
(config)#service timestamps log datetime msec
```

```
Enable terminal exec prompt timestamp for the debugging sessions
Router#terminal exec prompt timestamp
```

Troubleshooting DMVPN

- ❑ Check the GRE tunnels.

```
#show crypto isakmp sa
#show ip nhrp
```

```
#debug ip icmp
#debug ip packet
```

Cisco Easy VPN

- **Cisco Easy VPN** is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances.
- It greatly **simplifies VPN deployment** for remote offices and mobile workers.
- Cisco Easy VPN is based on the Cisco Unity[®] Client Framework, which centralizes VPN management across all Cisco VPN devices, thus **reducing the management complexity** of VPN deployments.
- Also, used for the **XAUTH** authentication.
- There are three components of the Cisco Easy VPN solution:
 - Easy VPN Client
 - Easy VPN Remote
 - Easy VPN Server

Cisco Group Encrypted Transport VPN (GETVPN)

- Is a method for creating a VPN without the management issues of provisioning a tunnel.

Cisco Secure Socket Layer VPN (SSLVPN)

- Is a technology that allows remote users to access the VPN using only the @Internet and a web browser.

Domain Name System (DNS)

```
(config)#ip dns server
(config)#ip host [RTR-1] [192.168.1.1]
(config)#ip dhcp excluded -address [x] [x]
```

```
no ip domain-lookup → Disable DNS service on the router.
```

Ping (ICMP)

- IP Header **1**.
- ICMP is a **protocol** and does not need TCP or UDP for transport.
- ICMP-Echo-Request is waiting **2 sec.** for a reply.
- If only one ICMP-Echo-Request fails, this indicates, that on one of the devices on the way, a **ARP-Entry was missing**.

On switches and routers, the **Extended-Ping** test is helpful to indicate problems on the way back of the packet.

- Depending from which interface you are testing, you will be able to test the Default-Gateway setting of a host.
- With ping you may also indicate DNS-Problems.

Interesting ICMP message types:

- **Destination unreachable**
- **Redirect**

```
#ping [IP]
#ping [IP] source loopback 0
```

Traceroute / Tracert

- Traceroute triggers errors on the router to report IP-Address of the router. The triggered error msg is ICMP Time to Live Exceeded.
- Each router reduces the TTL-Value in the header by minus one when the frame passes the router. If the TTL-Value is zero, the router drops the frame and sends a TT-Exceeded msg back to the sending host.
- The sender of the traceroute is increasing the TTL-Value one by one to follow the whole pass to the destination.
- Default TTL is **255**.

If you have more than one route to a destination device, the most precise route will be taken.

0.0.0.0/0 default route.

IPv4 Routing

Default-Gateway / Default-Router

If the receiving host is in the same network (Network-ID) the packet will be sent directly to the respective host, based on the MAC-Address of the receiving host. The MAC-Address of the receiving host will be evaluated with the Address Resolution Protocol(ARP).

The IP-Packet will be encapsulated in a Security-Layer Frame.

If the receiving host is not in the same network (Network-ID) than the IP-Packet will be sent to the Default-Gateway based on the Default-Gateways MAC-Address.

The Default-Gateway checks incoming Security-Layer Frames first upon errors (FCS-Field). The Default-Gateway compares than the Receivers-IP address with the internal routing table and forwards the packet through the respective interface to receiver host or the next hop.

Security-Layer Frame (2) can be Ethernet, High-Level Data Link Control(HDLC), Frame-Relay, PPP etc.

Point-to-Point-WANs

- Architecture type

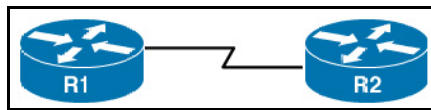


Figure 96: Point-to-Point Network Type

Leased Line (Serial Connection)

Similar to an Ethernet-Crossover-Cable (Router to Router)

The **connection clock** is on the **DCE-Side**.

- Uses protocol High-Level Data Link Control (**HDLC**)
- Or Point-to-Point Protocol (**PPP**)

Customer Premise Equipment (CPE)
Channel Service Unit/Data Service Unit (CSU/DSU)
Serial cable (EIA/TIA-232, V.35, X.21, DB-60)

T1 1.544 Mbps

PPP is using PAP and CHAP.

Overlay Transport Virtualization (OTV)

- OTV is a "MAC in IP" technique to extend Layer 2 domains over any transport.
- For DC interconnection.
- Needs PMTDU of **1542 Bytes** from point-to-point.
- Between OTV devices **IS-IS** is used.

OTV Devices:

Nexus 7000

CISCO PRODUCTS

Cisco Small Business RV180W - Wireless Router

1000:	Nicht aktualisierbar
2500:	Nicht aktualisierbar
2600:	End-of-live
28xx:	
29xx:	
2960-X:	Switch
35xx:	Layer 3 switch
3650:	Switch
37xx:	Layer 3 switch
3750-X:	Switch
3850:	Switch
4000:	ROM updateable
4500E	Switch
4500R	Catalyst
4500-X	Switch
550x	Adaptive Security Appliances (ASA)
WLC5760	
62xx:	Digital Subscriber Line Access Multiplexers (DSLAM)
65xx:	Layer 3 switch
6800	Catalyst
6807-XL	Switch
7500:	ROM updateable

CISCO ACS

Cisco Access Control Server

- Runs on a **Windows Server OS** also appliances are available.
- Is an **AAA** system.
- Policy-driven access control system and an integration point for network access control and identity management.
- Runs either on dedicated appliance or on a VMware server

CISCO DUO

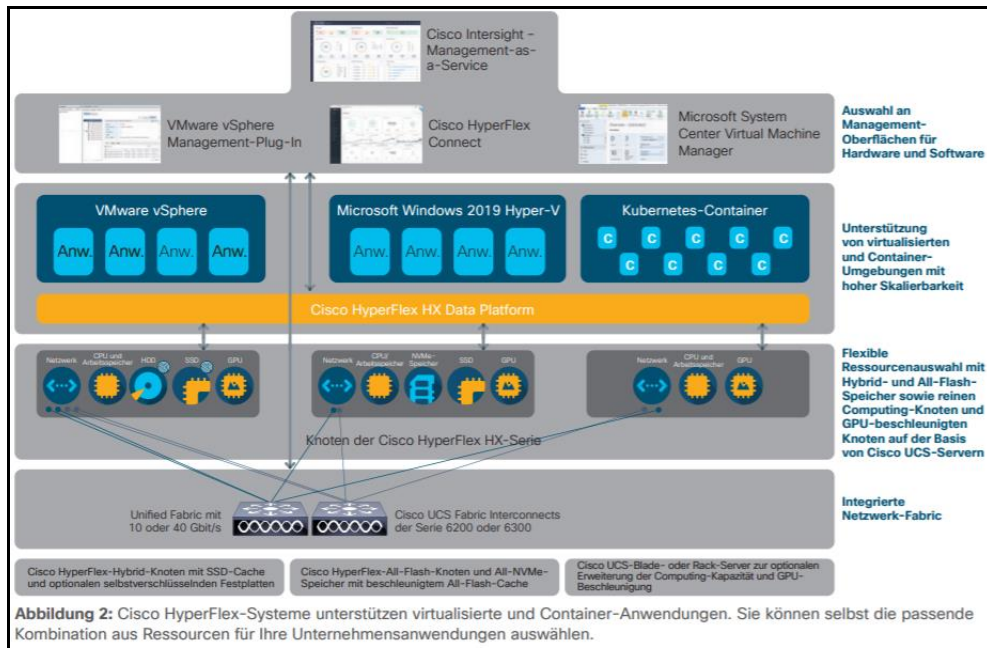
- Cisco, a worldwide leader in IT and networking, and **Duo** partner to bring **zero-trust security solutions** for joint customers.
- Duo and Cisco collaborate on range of use cases to bring strong user and device verification and mutual exchange of security context.
- The Duo-Cisco joint solution enables customers to deploy zero-trust security measures both inside and outside the corporate network.
- Duo's integration with **Cisco ASA VPN** provides strong user authentication and device security hygiene check and visibility. This integrated solution provides security admins the ability to enforce consistent **user and device based access policy for VPN access** and thereby reduce risk for data breaches and meet compliance requirements.
- Duo is **integrated with Umbrella** to provide strong user authentication, device security hygiene check and visibility thereby ensuring access to Umbrella is not compromised.
- Duo's integration with **Cisco WebEx** offers a variety of methods for adding two-factor authentication and flexible security policies to **WebEx SSO logins**. Duo layers strong authentication and a flexible policy engine on top of WebEx logins using the Security Assertion Markup Language (**SAML**) 2.0 authentication standard. Duo authenticates your users using existing on-premises or cloud-based directory credentials and prompts for **two-factor authentication before permitting access to WebEx**.

CISCO HyperFlex Systems (HX)

Cisco HyperFlex System

See: [Cisco Guide](#)

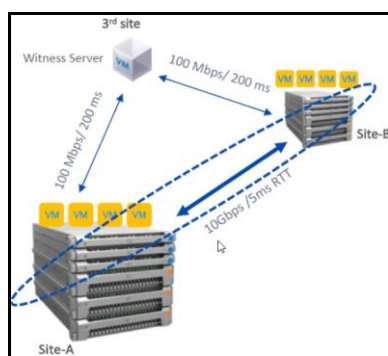
- HyperFlex is **Cisco's HCI platform**.
- A Cisco HyperFlex cluster contains a minimum of **three** converged HyperFlex nodes.
- Comes pre-installed with a distribution of **Kubernetes**.
- Adds container support with a new driver to provide persistent storage for **Kubernetes-managed containers**.
- Supports **Virtuelle Desktops (VDI)**.
- Supports several Hypervisors:
Microsoft Windows Server 2019 Hyper-V, VMware, vSphere, Docker-Container mit **Kubernetes**,



Cisco HyperFlex Systems Stretched Cluster

See: [Cisco Guide](#)

- A stretched cluster is a **single cluster** with **geographically distributed nodes**.
- For a "Cisco HyperFlex Systems Stretched Cluster" a **Witness Server** is required.



CISCO ISE

Cisco Identity Service Engine

- The new generation centralized policy engine for business-relevant policy definition and enforcement.
- Combines **Cisco ACS** and **NAC** solutions.

CISCO MERAKI

See: meraki.com

- Wireless management (Wifi)
- Mobile Device Management

Configuring Authentication Proxy:

```
#ip auth-proxy [NAME]
#ip auth-proxy auth-cache-time [min]
#ip auth-proxy auth-proxy-banner [TEXT]
#ip auth-proxy max-nodata-conns [x] → Max number of idle TCP connections.

#clear ip auth-proxy cache [* | IP]
#show ip auth-proxy
```

CISCO Prime

- Cisco Prime is a **network management software suite** consisting of different software applications by Cisco Systems.

CISCO Security MARS

Cisco Security Monitoring, Analysis and Response System.

- **Appliance.**
- **Identifying threats** on the Cisco network by "learning" the topology, configuration, and behavior of your environment.
- Making **precise recommendations** for threat mitigation, including the ability to visualize the attack path and identify the source of the threat.
- **Simplifying incident management** and response through integration with Cisco Security Manager security management software.

CISCO Stealthwatch

- Cisco Stealthwatch is the most comprehensive visibility and **network traffic security analytics** solution that uses enterprise telemetry from the existing network infrastructure.
- It provides **advanced threat detection**, accelerated threat response, and simplified network segmentation using multilayer machine learning and entity modeling.
- With advanced behavioral analytics, **you'll always know who is on your network and what they are doing.**
- A single, **agentless solution** allows visibility across the extended network, including endpoints, branch, data center, and cloud.
- And with **Encrypted Traffic Analytics**, Cisco Stealthwatch is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.

- Stealthwatch Management Console (SMC)
- Flow Collectors are needed
- Flow Sensors are needed

Features:

- ✓ Network traffic security analytics
- ✓ Advanced threat detection
- ✓ Encrypted Traffic Analytics

CISCO Umbrella

- To help organizations embrace direct internet access, in addition to **DNS-layer security** and interactive threat intelligence, Cisco Umbrella now includes **secure web gateway, firewall**, and

cloud access security broker (CASB) functionality, plus integration with **Cisco SD-WAN**, delivered from a single cloud security service.

Cisco IOS Command Reference (CLI)

See: http://www.cisco.com/c/en/us/td/docs/ios/fundamentals/command/reference/cf_book.html
http://www.cisco.com/c/en/us/td/docs/ios/12_2/configfun/command/reference/ffun_r.html
http://www.cisco.com/c/en/us/td/docs/ios/12_2/interface/command/reference/finter_r/irfusing.html
<http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/d1/sec-d1-cr-book/sec-cr-i1.html>

?	Help
!	Trennzeichen
q	Quit
cd	
[Enter]	Show line by line
[Spacebar]	Show rest
Ctrl+A	Beginn of the line
Ctrl+B	Back one character
Ctrl+C	Abort configuration, Exit
Ctrl+E	End of the line
Ctrl+F	Forward one character
Ctrl+N	Next
Ctrl+P	Previous Command
Ctrl+Z	Leave configuration mode, Exit
Ctrl+Shift+6	Interrupt a Cisco IOS process
Ctrl+Shift+6 X	Multiple active telnet sessions

*** A ***

access-class	→ Apply ACL to vty and controls (Remote access)
access-enable	
access-group	→ Assign ACL to Interfaces
access-list	→ Creates a standard numbered IPv4 ACL
access-list [x]	
access-list [x] deny host x.x.x.x	
access-list [x] deny tcp any host x.x.x.x eq 23 log	
access-template	
archive config	→ Creates a copy of the running-config to archive
arp -a	
auto-summary	- Summarize to classful boundary

*** B ***

bandwidth 64000	→ Definieren der Bandbreite 64 kbps
boot flash:[xxx.bin]	→ ROMmon mode
boot system rom	→ Booten von den ROM-Chips
boot system flash	→ Boots from first file on the FLASH-Memory
boot system [File] [IP-Adresse]	→ Booten vom Netzwerk

*** C ***

[no] cdp advertise-v2	→ Enables CDPv2
[no] cdp holdtime [sec]	
[no] cdp run	→ Enables CDP globally or for an certain interface
cdp timer 90	
channel-group 1 mode active passive	→ LACP
channel-group 1 mode auto desirable	→ PAgP

clear
clear arp
clear counters
clear counters s0/0/0
clear ip nat translations → NAT
clear line [x] → Disconnect telnet session

clock
clock timezone [x] [y] → Configure timezone
clock set [2:34:01] [21 august 2016] → Set time and date

cns

config-register
configure
configure memory
configure network
configure terminal

Ausführen im NVRAM gespeicherter Befehle.
Lokalisiert Befehle vom TFTP-Server.
→ Enter Global configuration mode

confreg → in ROMmon mode (rommon>)

connect

copy
copy running-config startup-config → RAM to NVRAM (overwrite it)
copy startup-config running-config → #Copy NVRAM to DRAM (Merge)

crypto key generate rsa → Generates a public and private key pair

***** D *****

debug

debug eigrp packets hello

debug ip nat → NAT real time translations

debug ipv6 ospf packet
debug ipv6 ospf hello

debug ppp
debug serial interface → Useful for HDLC encapsulation

debug standby → HSRP

default-information originate → RIP, OSPF
Imports a static default route.

delete
description [your description]
diagnostic
dir
dir all
disable → Leave privileged mode (EXEC-Mode)
disconnect

dot1x

[no] duplex full | half | auto → Configure interface

***** E *****

enable

enable password [pwd]

enable secret [pwd]

→ Start privileged mode (EXEC-Mode)

→ Should no longer be used

→ Set Password MD5 encrypted

encapsulation ppp

encapsulation dot1q [vlan]

encapsulation dot1q 1 native

→ Set encapsulation mode

→ Issue on Router for Inter-VLAN

→ Native means, not to add 802.1Q headers

Editor"

enter

Execute command(Is immediately active!) t

eou

erase

erase startup-config

→ Delete NVRAM

exec-timeout 0 0

exit

→ Set no timeout for password

→ Brings you back one level

***** F *****

***** G *****

***** H *****

hostname [hostname]

→ Set hostname

***** I *****

interface f0/1

interface loopback [0]

interface range f0/[1-xx]

→ Creates loopback interface [0]

ip address dhcp

ip address [ip] [mask]

ip address [ip] [mask] secondary

ip access-group [x] out | in

ip access-list extended [Name]

ip access-list standard [Name]

→ Obtain IP Address from ISP

→ On layer 2 switch address can only be set on VLAN 1

→

→ Apply ACL to an interface

ip cef

→ Advanced Layer 3 switching

ip default-gateway [ip]

→ Sets the default gateway

[no] ip domain-lookup

ip domain-name [name]

→ Dis-/Enables the translation of IP-Addresses on a router

→ Set domain name

ip flow ingress

ip flow egress

→ Incoming packets

→ Outgoing packets

ip flow-export destination [IP] [Port]

ip flow-export version 9

ip flow-export source loopback 0

→

→

→

ip forward-protocol nd	→ Forwards Network Disk(ND) packets
ip helper-address	→ Enable DHCP Relay Agent feature
ip host [routerx] [ip-address]	→ Define hosts table
ip mtu	→ Default 1500 Bytes 1514 also used frequently
ip nat pool	→ NAT
ip nat inside	→ Sets an interface to NAT inside
ip nat inside source static [ip] [ip]	
ip nat outside	→ NAT
ip nat <u>translation</u> max-entries	→ NAT
ip nat <u>translation</u> timeout	→ NAT
ip ospf cost	→ OSPF
ip ospf mtu-ignore	→ It's better to use the correct MTU values
ip proxy-arp	→ Enable Proxy ARP
ip route 0.0.0.0 0.0.0.0 fa0/0	
ip routing	→ Start Inter-VLAN routing
ip scp server enable	→ Secure Copy Protocol (SCP)
ip subnet-zero	
ip tcp window-size 65535	→ Enable window scaling.
ipv6 address auto-config default	→ IPv6 to use SLAAC
[no] ipv6 cef	
ipv6 enable	→ IPv6, Enables Automatic link-local address
ipv6 ospf [x] area [y]	
ipv6 router ospf [x]	
ipv6 unicast-routing	→ Enables ipv6 routing

*** **J** ***

*** **K** ***

*** **L** ***

license boot module	→ Disable active technology package
license call-home	→ Install a new license file (PAK)
license install	→ Install a new license file (not PAK)
line <u>console</u> 0	→ Console line configuration mode
line vty 0 4	→ Telnet VTY password, 0-4 five virtual lines
line vty 0 15	→ VTY port 0-15 connections
logging buffered	
logging host [ip]	
logging persistent url disk1:/syslog size [x] filesize [y]	
logging synchronous [5]	→ Logging synchronisation
logging traps [x]	

login → Require user password
login local → VTY configuration

***** M *****

mac address-table static [mac] vlan [x] int [x] → Creates a static MAC address

more flash:.vlan.dat

***** N *****

name [vName] → VLAN

network x.x.x.x
network [ip] [mask] area [x]

ntp master [x] → Sets stratum level to x

ntp peer [ip] → Receive clock and date information from NTP server
ntp server [ip-address] version 4

***** O *****

***** P *****

passive-interface FastEthernet 0/1 → Disables RIP on this interface
It suppresses sending routing updates out the interface

password [pwd]
ping <x.x.x.x>
ping ipv6 [] → IPv6

***** Q *****

***** R *****

reload → Reinitialize the switch

resume → Resumes the recent telnet session
resume [x] → Resumes the connection x

router ospf [x] → Enable OSPF process on x

router rip → RIP configuration

router-id x.x.x.x → OSPF

***** S *****

[no] service password-encryption

show access-lists
show access-lists interface

show archive → Backup settings

<u>show bootdisk</u>	→
<u>show buffers</u>	→ Checking buffer problems
<u>show cdp entry *</u>	→ Detailed Informations about neighboring devices
<u>show cdp entry * protocol</u>	→
<u>show cdp neighbors</u>	→ Shows only Layer 2 informations
<u>show cdp neighbors detail</u>	→ Shows also Layer 3 informations (IP)
<u>show clock</u>	
<u>show config</u>	→ Shows the content of the NVRAM's
<u>show control-plane host open-ports</u>	→ Shows open ports
<u>show controllers serial 0/0</u>	→ Show which type of cable is plugged in DTE/DCE
<u>show controllers s0/0</u>	
<u>show file systems</u>	→ Sows the IFS file system
<u>show flash</u>	→ Show IOS Flash (Privileged EXEC mode)
<u>show glbp</u>	→
<u>show glbp brief</u>	→
<u>show history</u>	→ Shows the last 10 commands entered
<u>show hosts</u>	→ Show hosts table
<u>show interfaces</u>	→ View configurable parameters Administrative status
<u>show interface brief</u>	→ Administrative status
<u>show interfaces access-lists</u>	
<u>show interfaces description</u>	
<u>show interfaces Fa0/15 switchport</u>	
<u>show interfaces status</u>	
<u>show interface trunk</u>	→ Shows: The VLANs allowed on the trunk The encapsulation method used for the trunk The interfaces which are trunks The native VLAN The administrative mode used to form the trunk
<u>show interfaces vlan 1</u>	→ Cmd not supported on routers.
<u>show ip arp</u>	→ Dash(-) = Physical interface
<u>show ip cef [ip]</u>	→ Displays the FIB
<u>show ip cache flow</u>	→ NetFlow Shows a summary of the NetFlow accounting statistics. Shows: Hardware flows and software flows Shows: Usage by protocol.
<u>show ip dhcp binding</u>	→ Shows host and allocation of IP
<u>show ip dhcp conflict</u>	
<u>show ip dhcp database</u>	→ Database agent informations such as: - Location - Status of connectivity
<u>show ip dhcp pool [x]</u>	→ Shows total numbers of addresses leased
<u>show ip dhcp server statistics</u>	→ Troubleshoot DHCP
<u>show ip eigrp topology</u>	→ Show all FS
<u>show ip flow top-talkers</u>	→
<u>show ip flow interface</u>	→
<u>show ip flow export</u>	→

<u>show ip interface</u>	→ Shows: - IP address and subnet mask - ACL name or number - Status and protocol status - The DHCP relay agent
<u>show ip interface brief</u>	→ Status: admin-down / down means - Data link layer does not work - Remote keepalive messages are not being received
<u>show ip nat translations</u> <u>show ip nat statistics</u>	→ Show NAT translation table → Summary of the NAT configuration Counters for packets and NAT table entries
<u>show ip ospf</u> <u>show ip ospf database</u> <u>show ip ospf interface [x]</u> <u>show ip ospf neighbor</u>	→ Shows: - OSPF Router ID → Router s in the AS and the neighbors
<u>show ip protocols</u>	→ Actual operation of all running protocols RIP Hold Down Timers
<u>show ip rip neighbors</u>	→ Shows RIP neighbors No Display Timers
<u>show ip route</u>	→ S = Static O = OSPF internal routes IA = OSPF inter area N1 = OSPF NSSA external Type-1 N2 = OSPF NSSA external Type-2 E1 = OSPF external Type-1 E2 = OSPF external Type-2 C = Directly connected networks B = BGP D = EIGRP EX = EIGRP external L = Local (/32) R = RIP I = IGRP M = Mobile E = EGP I = IS-IS L1 = IS-IS level-1 L2 = IS-IS level-2 U = per-user static route o = ODR
<u>show ip route [ip]</u> <u>show ip route connected</u> <u>show ip route ospf</u> <u>show ip route static</u>	→ Show effective route → → OSPF → Static routes
<u>show ipv6 access-lists</u> <u>show ipv6 eigrp topology</u> <u>show ipv6 int</u> <u>show ipv6 int brief</u> <u>show ipv6 int [int]</u> <u>show ipv6 neighbors</u> <u>show ipv6 ospf</u> <u>show ipv6 protocols</u>	→ IPv6 → IPv6 → IPv6 → IPv6 → IPv6 → IPv6 → IPv6

<u>show</u> ipv6 route	→ IPv6
<u>show</u> ipv6 route static	→
<u>show</u> ipv6 route ospf	→
show ipx route	→ IPX routing table
<u>show</u> license	→ show the activated Licenses
<u>show</u> license feature	→ Summarized show license
<u>show</u> lldp neighbors	
<u>show</u> log	
<u>show</u> mac address-table	→ Shows the forward/filter table DYNAMIC = STATIC =
<u>show</u> memory scan	
<u>show</u> ntp status	→ Reference master for the client
<u>show</u> ntp <u>a</u> ssociations	→ ref clock 127.127.1.1 = local clock source ref clock .LOCL. = local clock
<u>show</u> port-security	→ Shows violations
<u>show</u> port-security interface [if]	→ Shows violations
<u>show</u> processes	→ CPU utilization etc.
<u>show</u> processes cpu	
<u>show</u> protocols [IF]	
<u>show</u> privilege	
<u>show</u> <u>r</u> unning-config	→ Comes from RAM Shows all configuration settings such as: SCP,
<u>show</u> <u>r</u> unning-config interface [IF]	→ Shows all configuration settings for the specific IF.
<u>show</u> sessions	→ Show active telnet sessions The line with the (*) is the most recently used connection
<u>show</u> spanning-tree	→ root bridge, root ports and designated and blocking/discarding ports
<u>show</u> spanning-tree [Vlan_ID]	
<u>show</u> spanning-tree summary	
<u>show</u> standby	→ HSRP
<u>show</u> standby brief	→ HSRP
<u>show</u> <u>s</u> tartup-config	
<u>show</u> standby	
<u>show</u> tech-support	→ Shows password and user settings
<u>show</u> terminal	→ Shows the terminal history size
<u>show</u> trunk	→ SWITCH: Show trunk informations
<u>show</u> users	→ Console connections and remote connections
<u>show</u> version	→ Shows amount of Flash and DRAM DRAM = ... with 45056K/4096K bytes of memory

Flash = **32768K** bytes of processor ...
Shows **uptime** .
Configuration Register Values:
0x2102 = Factory default (IOS Flash Memory)
0x2100 = ROM monitor mode
0x2142 = ROM monitor mode (reset Pwd)

<u>show</u> vlan	→ Shows only access ports!
<u>show</u> vlan brief	→ Shows only access ports!
<u>show</u> vtp status	→ VLAN Trunk Protocol
[no] shutdown	
[no] speed [x]	→ Set speed of line
ssh -l [user] [ip]	→ SSH connection to another router
standby [group] ip [ip-address]	→ HSRP
standby [group] priority [priority]	→ HSRP, Higher Priority wins
standby [group] preempt	→ HSRP
standby [group] track [interface]	→ HSRP
spanning-tree portfast	
spanning-tree portfast default	→ Enable PortFast on all non-trunking ports
spanning-tree portfast bpduguard default	
spanning-tree portfast bpduguard enable	
spanning-tree vlan 2 priority [x 4096]	
spanning-tree vlan 3 root primary	
standby 1 ip 10.1.1.10	→ HSRP
<u>switchport</u> access vlan [x]	
<u>switchport</u> mode access trunk	→ Sets the port to mode <u>access</u>
<u>switchport</u> mode dynamic auto desirable	
<u>switchport</u> nonegotiate	→ No DTP frames
<u>switchport</u> port-security	→ Enables port security
[no] <u>switchport</u> port-security [mac]	→ Remove the MAC address from port security
<u>switchport</u> port-security mac-address sticky	→ Saves dyn. learned MAC addresses to the running-conf
<u>switchport</u> port-security maximum 1	→ Max. no of MAC addresses allowed on the interface
<u>switchport</u> port-security violation shutdown	→ Disables the port if a violation is detected
<u>switchport</u> trunk allowed vlan [1,2,...]	→ Set VLANs for a port
<u>switchport</u> trunk encapsulation dot1q	
<u>switchport</u> trunk native vlan [x]	→ Changes the default VLAN 1 to x
<u>switchport</u> voice vlan [x]	

***** T *****

telnet [ip-address]	
[no] terminal monitor	→ telnet
[no] terminal ip netmask-format decimal	→ Changes the netmask format from CIDR to x.x.x.x

traceroute

transport input telnet
transport input ssh
transport input telnet ssh

→ Only Telnet
→ (config-line)# Only SSH
→ (config-line)# Telnet and SSH

*** U ***

un all
username [name] password [pwd]

→ Turn off all debugging

*** V ***

version 1|2
verifz &md5 flash>\file|
vlan [0-4094]

→ RIP
→ VLAN

*** W ***

#wr mem

→ Write memory command

*** X ***

*** Y ***

*** Z ***

Routing Protocol Configurations (config-router)

router rip
ip routing

CDP

show cdp neighbors [typ nummer]
show cdp neighbors detail
show cdp entry name

Interfaces

interface fastEthernet 0/1
show interfaces status
show interfaces [typ] x switchport
show interfaces tunnelx

MAC

show mac address-table dynamic

ACL (config-std-nacl)

ip access-list standard ABO
show access-lists
show ip access-lists

GRE

interface tunnel
tunnel source
tunnel destination

EIGRP

show ip eigrp interfaces
show ip eigrp topology

CISCO Commands:

ip forward-protocol udp
ip route 150.1.0.0 120.1.1.2
modem inout
router igrp 9
sein.)
show controllers serial 0
show ip arp
show line [1]
terminal history xx
variance 1.5
write erase
write mem
write net
write terminal

Weiterleiten der Broadcast SLARP für Konfiguration
Definieren einer static-route.
Gibt die asynchrone Schnittstelle am router frei.
Aktivieren von IGRP (Nummern einer autonomen Gruppe müssen gleich
Zeigt die ARP-Tabelle (IP-Adresse + MAC-Adresse)
Zeigt Sende und Empfangsgeschwindigkeit.
Anzahl aufzuzeichnender Befehle (DOSKEY)
Lastenausgleich der Routen.
Eine Routerkonfiguration komplett zurücksetzen.
Schreibt die aktuell Konfiguration in das NVRAM.
Shows the configuration of the NVRAM on the screen.

Standard: Latency

One-way latency or round-trip time.

In telecommunications, the **round-trip delay time (RTD)** or **round-trip time (RTT)** is the length of time it takes for a **signal to be sent plus the length of time it takes for an acknowledgment (receive)** of that signal to be received. It's also called **ping time**.

Latency for SAP

Max. recommended latency for SAP is 350 ms

Latency for MS Dynamics AX / Axapta

Max. recommended latency for Axapta is 150 ms

Latency for MS Navision (NAV)

Max. recommended latency for Navision is 200 ms

Latency for VoIP

Max. recommended one-way latency according G.114 is 150 ms

Tools: Looking Glass (@Internet)

To receive information's about routing in the @Internet.
Helps you in case your ISP has a problem!

Links: <http://www.lookingglass.org>
https://www.bgp4.net/doku.php?id=tools:ipv4_looking_glasses

NETWORK TECHNIQUES

464XLAT

464XLAT (RFC 6877) allows clients on IPv6-only networks to access IPv4-only @Internet services, such as Skype.

Source: Wikipedia

Address Resolution Protocol (ARP)

The Address Resolution Protocol is used to dynamically discover the **mapping between a layer 3 (protocol) and a layer 2 (hardware) address**. A typical use is the mapping of an IP address (e.g. 192.168.0.10) to the underlying Ethernet address (e.g. 01:02:03:04:05:06). You will often see ARP packets at the beginning of a conversation, as ARP is the way these addresses are discovered.

ARP can be used for Ethernet and other LANs, ATM, and a lot of other underlying physical addresses (the list of hardware types in the **ADDRESS RESOLUTION PROTOCOL PARAMETERS** document at the IANA Web site includes at least 33 hardware types).

ARP is used to dynamically build and maintain a mapping database between link local layer 2 addresses and layer 3 addresses. In the common case this table is for mapping Ethernet to IP addresses. This database is called the ARP_Table. Dynamic entries in this table are often cached with a timeout of up to **15 minutes**, which means that once a host has ARPed for an IP address it will remember this for the **next 15 minutes** before it gets time to ARP for that address again.

A peculiarity of ARP is that since it tries to reduce/limit the amount of network traffic used for ARP a host MUST use all available information in any ARP packet that is received to update its ARP_Table. Thus, sometimes a host sends out ARP packets NOT in order to discover a mapping but to use this side effect of ARP and preload the ARP table of a different host with an entry. These special ARP packets are referred to as **Gratuitous_ARPs** and Wireshark will detect and flag the most common versions of such ARPs in the packet summary pane.

Gratuitous_ARPs are more important than one would normally suspect when analyzing captures. So, don't just ignore them or filter out ARP from your capture immediately. Consider that a normal host will always send out a Gratuitous_ARP the first thing it does after the link goes up or the interface gets enabled, which means that almost every time we see a Gratuitous_ARP on the network, that host that sent it has just had a link bounce or had its interface disabled/enabled. This is very useful information when troubleshooting networks. Remember though that you can only see these Gratuitous_ARPs (or any other ARPs for that matter) if your capture device is in the same Broadcast Domain as the host that originates the ARP packet.

Several viruses send a lot of ARP traffic to discover hosts to infect; see the **ArpFlooding** page.

Source: Wireshark

Akamai Technologies Inc.

deploy.akamaitechnologies.com

Is a cloud services provider headquartered in Cambridge, Massachusetts, in the United States. Akamai's content delivery network is one of the world's largest distributed computing platforms. The company operates a network of servers around the world and rents capacity on these servers to customers who want their websites to work faster by distributing content from locations close to the user. Over the years their customers have included Facebook, Bing, Twitter and healthcare.gov. When a user navigates to the URL of an Akamai customer, their browser is redirected to one of Akamai's copies of this website, almost entirely invisible to the vast majority of its users.

Source: Wikipedia

APNIC

- APNIC maintains a **database (WHOIS)** of all registered IP address blocks and information about who is using this address space in Asian Pacific.

- When an ISP allocates address space to another company, it registers this allocation by sending an APNIC report to Whois.

Archie

- FTP search protocol.
- Is used to search FTP sites for files.
- ARCHIE is used to search for files that are cataloged on ARCHIE servers, which are spread over the entire @Internet.

ArcNet

- Arcnet transmits at only 2.5 Mbps, but the new ArcNet Plus can transmit at up to 20 Mbps.
- Token Passing access method
- Each ArcNet packet contains a source address, a destination address, and up to 508 bytes of Data for ArcNet or up to 4,096 bytes of data for ArcNet Plus
- Coaxial Cable / Star / 2000 feet max. dist. From computer to Hub
- Coaxial cable / Bus / 1000 feet max. dist. From computer to Hub
- UTP / Star / 800 feet max. dist. From computer to Hub
- UTP / Bus / 800 feet max. dist. From computer to Hub

Autonomous System Number (ASN).

RFC 5398

Within the @Internet, an **Autonomous System (AS)** is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the @Internet.

Originally the definition required control by a single entity, typically an Internet service provider or a very large organization with independent connections to multiple networks, that adhere to a single and clearly defined routing policy, as originally defined in RFC 1771. The newer definition in RFC 1930 came into use because multiple organizations can run BGP using private AS numbers to an ISP that connects all those organizations to the @Internet. Even though there may be multiple Autonomous Systems supported by the ISP, the @Internet only sees the routing policy of the ISP. That ISP must have an officially registered **Autonomous System Number (ASN)**.

Source: Wikipedia

- An **autonomous system** is a collection of routers that are under a common administrative control (e.g. ISPs).
- Each company whose enterprise network connects to the **@Internet** can be considered to be an autonomous system and can be assigned a BGP ASN.
- The 16-bit BGP ASN implies a decimal range of 0 - 65'535

0	Reserved
1 - 64495	Public ASNs
64496 - 64511	Reserved for BGP Documentation
64512 - 65534	Private ASNs
	Or 64086.59904 - 65535.65534
65535	Reserved

Swisscom (Switzerland)	AS 3303
Liberty Global Operations (Cablecom)	AS 6830
Sprint	AS 1239

Tools: <https://www.ultratools.com/tools/asnInfo>

Interesting AS nos

AS 3356	Level 3
AS 4637	Telstra Global
AS 8075	MICROSOFT
AS 12510	Internet Services SAP AG
AS 13353	Telmex do Brasil
AS 15169	GOOGLE
AS 20940	AKAMAI - ASN1 Akamai International B.V., US
AS 33891	Core-Backbone GmbH

Broadcast Domain

A **broadcast domain** is a logical division of a computer network, in which all nodes can reach each other by broadcast at the **data link layer**. A broadcast domain can be within the same LAN segment or it can be bridged to other LAN segments.

In terms of current popular technologies: Any computer connected to the same Ethernet **repeater** or **switch** is a member of the same **broadcast domain**. Further, any computer connected to the same set of inter-connected switches/repeaters is a member of the same **broadcast domain**. **Routers** and other higher-layer devices form boundaries between **broadcast domains**.

This is as compared to a **collision domain**, which would be all nodes on the same set of inter-connected repeaters, divided by switches and learning bridges. Collision domains are generally smaller than, and contained within, broadcast domains.

Source: Wikipedia

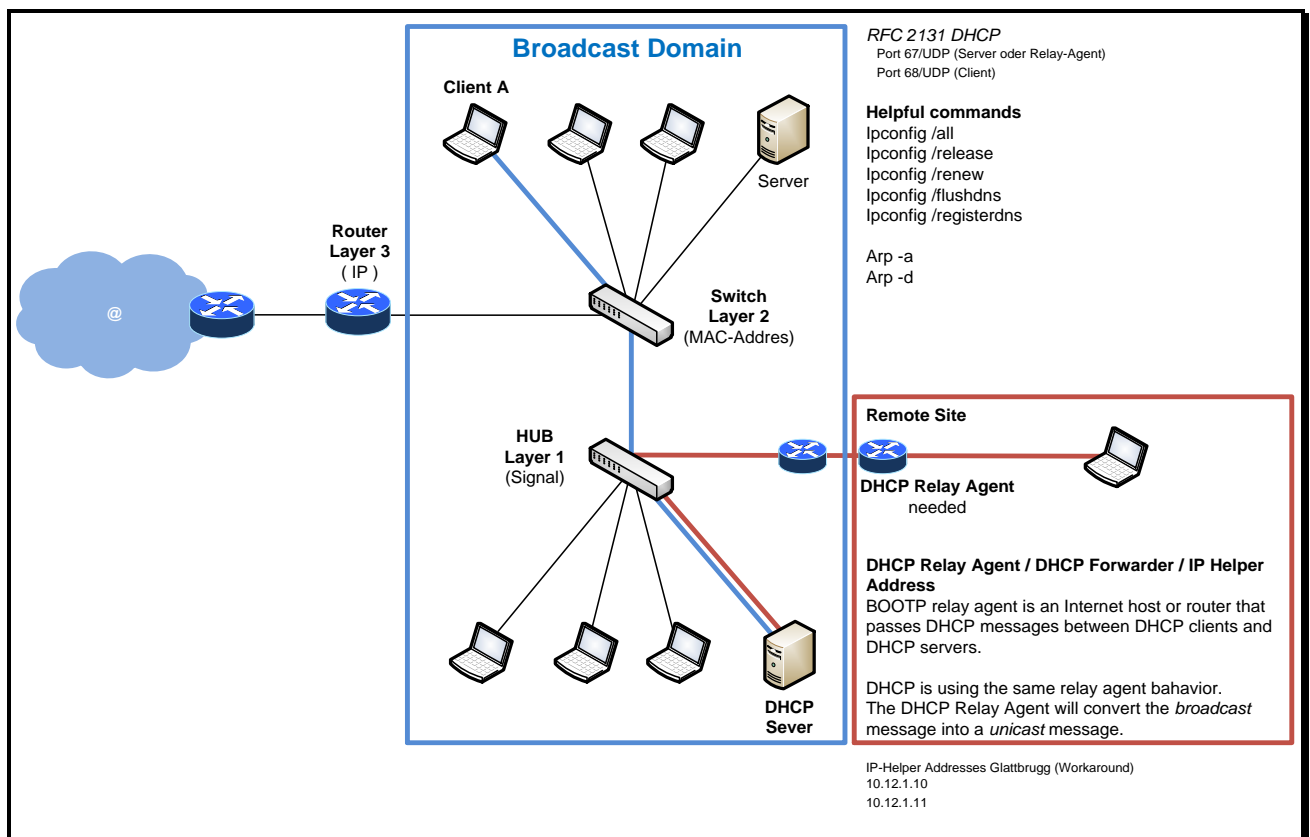


Figure 97: Broadcast Domain

CAPWAP

The **Control And Provisioning of Wireless Access Points (CAPWAP)** protocol is a standard, interoperable networking protocol that enables a central wireless LAN *Access Controller (AC)* to manage a collection of *Wireless Termination Points (WTPs)*, more commonly known as Wireless Access Points. The protocol specification is described in RFC 5415.

Source: Wikipedia

Certificate Types

Self Signed Certificates

For internal purposes

Domain Validated Certificate

The only verification check which is performed, is to ensure that the application owns the domain.

FULLY AUTHENTICATED SSL CERTIFICATES

Wildcard Certificates

Provides full SSL security to any host of your domain e.g. <host>.<domain>.com

Subject Alternative Name (SAN) Certificate

Single certificate for more than one domain.

Extended Validation Certificate (EV SSL)

Highest industry standard for authentication.

Certificate Authority (CA)

In cryptography, a certificate authority or certification authority (CA), is an **entity that issues digital certificates (SSL)**. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. CAs are characteristic of many public key infrastructure (PKI) schemes.

Source: Wikipedia

Your selected CA should provide support for both Certificate Revocation List (CRL) and Online Certificate Status Protocol (OCSP). **OCSP Stapling** is a modification of the OCSP protocol that allows revocation information to be delivered as part of the TLS handshake, directly from the server to the browser (see Performance)

Private Key and Certificate

- **Use 2048-bit Private Keys** - The bigger the private key the harder it is to crack, but the more computing resources it's going to take. For now, at least a 2048-bit private key is recommended for optimum security.
- **Protect Private Keys** - Make sure you create your own private keys on a secure and trusted computer. Only give access to private keys as needed. When an employee with private key access leaves your company, generate a new private key.
- **Choose a Reliable Certification Authority (CA)** ~ If you choose a reliable Certificate Authority - like [SSL.com](#) - you can rest assured that your private key and SSL certificate are going to work to protect data being transferred to and from your server.

System Configuration

Next up is a list of some of the best practices for configuring your system to use the SSL certificate. The Forward Secrecy protocol may require some extra work, but we'll have more on that below.

- **Valid Certificate Chains** - In cases where you have two or more certificates, you should ensure that the entire certificate chain is set up properly. Even if everything is installed correctly, you may have one SSL certificate that expires before others, which could corrupt the entire chain.
- **Use Secure Protocols** - Ensure that you are using TLS v1.1 and v1.2. As you know, SSL 3.0 support is quickly disappearing from the web ever since Google announced problems with a POODLE attack.
- **Secure Cipher Suites** - Choose your cipher suites carefully. Some are more secure than others. You should choose only the ones that offer 128 bits protection - stronger when possible. While 3DES (symmetric) may be close enough at 112 bits, it's slow and shouldn't be used.
- **Forward Secrecy Protocol** - This can allow you to enable secure connections not dependent on a private key. You will need to support and prefer ECDHE cipher suites for this to work correctly, but it's worth the effort.
- **Client-Initiated Renegotiation** - While the server may need to renegotiate a connection, a client will NOT need this access, so make sure it is disabled. If you don't, it can make your server more susceptible to DDoS attacks.
- **Disable SSLv3** - Thanks to the POODLE vulnerability, you should disable SSLv3 and stop using it immediately. Chrome and other web browsers have already removed support for SSL v3 because of security concerns. Make sure and disable SSL 3.0 sessions entirely if you are

using an older browser. Chrome and other web browsers have already removed support for SSLv3 in their newest versions because of security concerns, so updating your browser is also an excellent idea to help deal with these issues from the client side.

- **New Vulnerability Alerts** - Most importantly, you should always be on the lookout for the next attack. This means reading and staying in touch with what's on the horizon when it comes to information security as well as keeping on top of software updates - especially the critical ones. The best place to do this? Here at Info.SSL.com, of course. We'll keep you up to date on everything you need to know about SSL and information security.

Cipher

- SSLCipherSuite
- RC4 cipher is insecure and should be disabled.
BEAST and "Lucky Thirteen"

Cisco Application Visibility and Control (AVC)

The Cisco Application Visibility and Control (AVC) solution is a suite of services in Cisco network devices that provides application-level classification, monitoring, and traffic control, to:

- Improve business-critical application performance
- Support capacity management and planning
- Reduce network operating costs

Cloud Solution

- Scalable IT-Infrastructure
- Installation free
- Maintenance free

Public Cloud

Accessible for everyone.

Private Cloud

Because of data protection and IT-Security the service is accessible only for internals.

Hybrid Cloud

Use of Public Cloud services together with Private Cloud services.

The important thing is to distinguish which data has to be protected (Private Cloud)

Community Cloud

A kind of Private Cloud, but for several companies. They share the environment but only for their internals

Collision Domain

A **collision domain** is a section of a network where data packets can collide with one another when being sent on a shared medium or through repeaters, particularly when using early versions of Ethernet. A network collision occurs when more than one device attempts to send a packet on a network segment at the same time. Collisions are resolved using carrier sense multiple access with collision detection (**CSMA/CD**) in which the competing packets are discarded and re-sent one at a time. This becomes a source of **inefficiency in the network**.

Only one device in the collision domain may transmit at any one time, and the other devices in the domain listen to the network in order to avoid data collisions. Because only one device may be transmitting at any one time, total network bandwidth is shared among all devices. Collisions also decrease network efficiency on a collision domain; if two devices transmit simultaneously, a collision occurs, and both devices must retransmit at a later time.

Since data bits are propagated at a finite speed, simultaneously is to be defined in terms of the size of the collision domain and the minimum packet size allowed. A smaller packet size or a larger dimension would make it possible for a sender to finish sending the packet without the first bits of the message being able to reach the most remote node. So, that node could start sending as well, without a clue to the transmission already taking place and destroying the first packet. Unless the size of the collision domain allows the initial sender to receive the second transmission attempt - the collision - within the

time it takes to send the packet he would neither be able to detect the collision nor to repeat the transmission - this is called a late collision.

Collision domains are found in a **hub** or **repeater** environment where each host segment connects to a hub that represents only one collision domain within one broadcast domain. Collision domains are also found in other shared medium networks, e. g. wireless networks such as Wi-Fi.

Modern wired networks use a network **switch** to eliminate collisions. By connecting each device directly to a port on the switch, either each port on a switch becomes its own collision domain (in the case of half duplex links) or the possibility of collisions is eliminated entirely in the case of full duplex links.

Source: Wikipedia

CSR-File Extension

A file with the CSR file extension is usually a **Certificate Signing Request** file.

What is a CSR? A CSR or Certificate Signing request is a block of encrypted text that is generated on the server that the certificate will be used on. It contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR.

How do I generate a CSR and private key?

You need to generate a CSR and private key on the server that the certificate will be used on. You can find instructions in your server documentation or try the instructions from one of these certificate authorities:

[Comodo CSR Generation Instructions](#)

[DigiCert CSR Generation Instructions](#)

[GeoTrust CSR Generation Instructions](#)

[Thawte CSR Generation Instructions](#)

[VeriSign CSR Generation Instructions](#)

If you are familiar with OpenSSL you can use the following command to generate a CSR and private key:

See: **www.openssl.org**

```
openssl req -new -keyout server.key -out server.csr
```

Dark Fibre

- A **dark fibre** or **unlit fibre** is an unused optical fibre, available for use in fibre-optic communication.
- The term *dark fibre* was originally used when referring to the potential network capacity of telecommunication infrastructure, but now also refers to the increasingly common practice of leasing fibre optic cables from a network service provider, or, generally, to the fibre installations not owned or controlled by traditional carriers.

Source: Wikipedia

Denial-of-Service (DoS)

- In computing, a **denial-of-service (DoS)** or **distributed denial-of-service (DDoS)** attack is an attempt to make a machine or network resource unavailable to its intended users.

DNSBL

Also called Real-time Blackhole List (RBL).

List of IP addresses which are most often used to publish the addresses of computers or networks linked to **spamming**; most mail server software can be configured to reject or flag messages which have been sent from a site listed on one or more such lists. The term "Blackhole List" is sometimes interchanged with the term "blacklist" and "blocklist".

Source: Wikipedia

Popular Blacklist sites:

Spamcop.net

Tool: <http://mxtoolbox.com/blacklists.aspx> to check if your server is blacklisted.

Process: To whitelist from RBL

DNS Round Robin load balancing

Busy web-sites often use multiple web-servers in order to handle traffic load. Traffic can be distributed (load balanced) between such web-servers using DNS round robin. The DNS server simply rotates the DNS records for each incoming DNS request, resulting in each visitor being served by a different web-server. However, DNS round robin in itself does not provide any failover functionality.

If one of the web-servers fail, some visitors will still be directed to the failed server because of the **round robin** list:

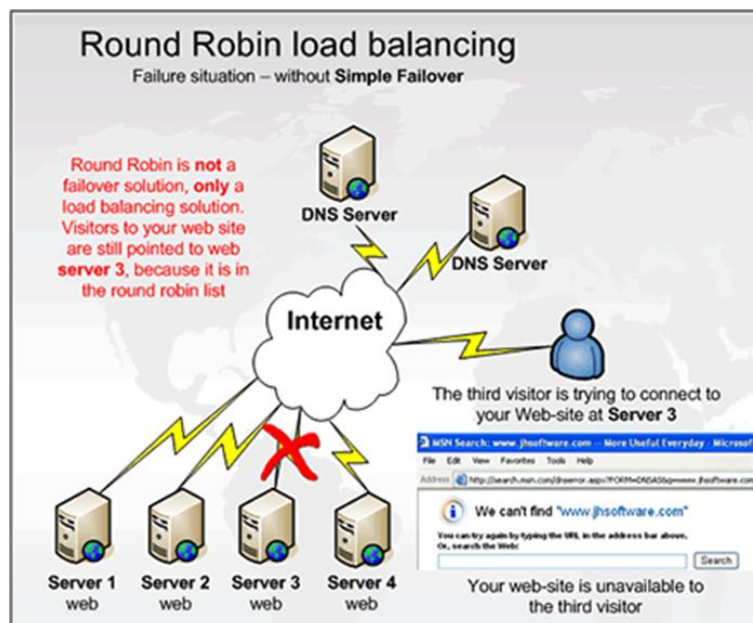


Figure 98: DNS Round Robin

Domain Name System Security Extensions (DNSSEC)

The **Domain Name System Security Extensions (DNSSEC)** is a suite of Internet Engineering Task Force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) as used on Internet Protocol (IP) networks. It is a set of extensions to DNS which provide to DNS clients (resolvers) **origin authentication of DNS data**, authenticated denial of existence, and data integrity, but not availability or confidentiality.

Source: Wikipedia

- DNSSEC-compliant DNS servers use **HSM** for **key** and **zone file storage**.

Dynamic DNS (DDNS)

???

ECHELON

NSA is controlling since 1980 communications.

Economic Operators Registration and Identification (EORI) System

The Economic Operators Registration and Identification (EORI) System, an EU-wide scheme for the registration and identification of companies, was introduced in November 2009. The identification

number consists of a customs number preceded by a two-digit country code (e.g. IT1234567). The EORI master data (which corresponds to the ATLA master data) is saved in the central EU database. In accordance with data protection regulations, the economic operator has to provide written permission for this retention of data. If you previously had a customs number, you should have been informed about the EORI regulations by the customs authorities in the form of a letter. Further information is available here:

http://ec.europa.eu/ecip/security_amendment/who_is_concerned/index_en.htm#eori

Enhanced Data rates for GSM Evolution (EDGE)

(also known as Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution) .

Is a digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM. EDGE is considered a pre-3G radio technology and is part of ITU's 3G definition. EDGE was deployed on GSM networks beginning in 2003 - initially by Cingular (now AT&T) in the United States.

Source: Wikipedia

Fibre Channel (FC)

Is a high-speed network technology (commonly running at 2-, 4-, 8- and 16-Gbps rates) primarily used to connect computer data storage.

Source: Wikipedia

Fibre Channel over Ethernet (FCoE)

Transmission of Fibre Channel frames over Ethernet.

See also "Data Center Bridging".

File Systems

NFS	Network File System
SMB/CIFS	Server Message Block/Common Internet File System

Frame Relay

See: Communication General.docx

FTP

- Is a protocol used on the Internet to browse and to transfer files from one site to another.
- FTP is an application layer protocol that is widely used for transferring large text and binary files.

FTPS

FTPS (also known as FTP-ES, FTP-SSL and FTP Secure) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols.

FTPS should not be confused with the SSH File Transfer Protocol (SFTP), an incompatible secure file transfer subsystem for the Secure Shell (SSH) protocol. It is also different from FTP over SSH, the practice of tunneling FTP through an SSH connection.

Source: Wikipedia

Gopher

- Gopher is a menu-based system for searching the @Internet and transferring files from various sources according to their relation to a particular topic.
- Gopher servers exist throughout the Internet, and they are linked together through distributed indexes that are collectively known as **Gopherspace**.
- Gopher has a search engine called **VERONICA**, which is the equivalent of the FTP search engine ARCHIE. Gopher sites can also be searched using another search engine called the **Wide Area Information Server (WAIS)**.

High-Speed Downlink Packet Access (HSDPA)

Is an enhanced 3G (third-generation) mobile-telephone communications protocol in the High-Speed Packet Access (HSPA) family, also dubbed 3.5G, 3G+ or turbo 3G, which allows networks based on Universal Mobile Telecommunications System (UMTS) to have higher data-transfer speeds and capacity. As of 2013 HSDPA deployments can support down-link speeds of up to 42.2 Mbit/s. HSPA+ offers further speed increases, providing speeds of up to 337.5 Mbit/s with Release 11 of the 3GPP standards.

Source: Wikipedia

High-Speed Uplink Packet Access (HSUPA)

Is a 3G mobile telephony protocol in the HSPA family with up-link speeds up to **5.76 Mbit/s**. The name HSUPA was created by Nokia. The official 3GPP name for 'HSUPA' is Enhanced Uplink (EUL).

Source: Wikipedia

HTML

- Is a standard for defining documents with hypertext links.
- HTML v2.0 was defined by the **Internet Engineering Task Force (IETF)** with the basic features for all WWW documents.

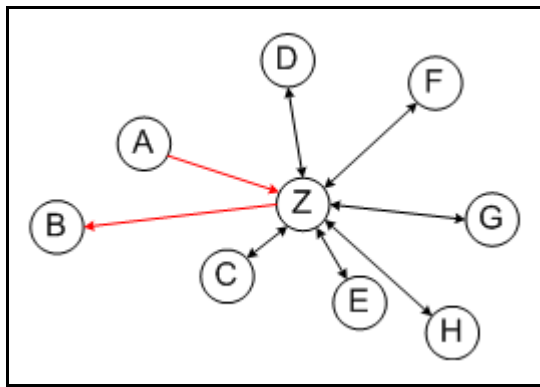
HTTP

HTTP 1.1
RFC 2068

HTTP 2.0, HTTP/2, HTTP/2.0
RFC 7540
Compatible with HTTP 1.1 but increased speed (See SPDY-Technique).

Hub and Spoke

If the way from A to B is through Z, we are talking about "Hub and Spoke".



IBM Websphere Application Server (WAS)

is a software product that performs the role of a **web application server**. More specifically, it is a software framework and **middleware** that hosts Java based web applications. It is the flagship product within **IBM's WebSphere software suite**.

Source: Wikipedia

Internet Relay Chat (IRC)

is an application layer protocol that facilitates communication in the form of text. The chat process works on a client/server networking model. IRC clients are computer programs that a user can install on their system. These clients communicate with chat servers to transfer messages to other clients. IRC is mainly designed for group communication in discussion forums, called channels, but also allows one-on-one communication via private messages as well as chat and data transfer, including file sharing.

Client software is available for every major operating system that supports @Internet access. As of April 2011, the top 100 IRC networks served more than half a million users at a time, with hundreds of

thousands of channels operating on a total of roughly 1,500 servers out of roughly 3,200 servers worldwide.

Over the past decade IRC usage has been declining: since 2003 it has lost 60% of its users (from 1 million to about 400,000 in 2014) and half of its channels (from half a million in 2003).

Source: Wikipedia

Internet Content Adaption Protocol (ICAP)

- Protocol to execute “Remote Procedure Calls” for HTTPS & FTP.
- Works with a ICAP-Server.
- ICAP-Client is usually a Proxy.

IoT - Skydrive and Rackspace Cloud. Internet of Things

- The connection of **physical things** to the @Internet makes it possible to access remote sensor data and to control the physical world from a distance.
- See it in conjunction with techniques like Wearables, RFID, IPv6
- IoT makes use of the **UcIP** stack.

Prediction: **10 IP's per person**

ISATAP

RFC 5214

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 transition mechanism meant to transmit IPv6 packets between dual-stack nodes on top of an IPv4 network.

Unlike 6over4 (an older similar protocol using IPv4 multicast), ISATAP uses IPv4 as a virtual nonbroadcast multiple-access network (NBMA) data link layer, so that it does not require the underlying IPv4 network infrastructure to support multicast.

ISATAP defines a method for generating a link-local IPv6 address from an IPv4 address, and a mechanism to perform Neighbor Discovery on top of IPv4.

Source: Wikipedia

Disable ISATAP

Start → Run → <devmgmt.msc>

Show the hidden devices: View → Show hidden devices



Jumbo Frames

In computer networking, **jumbo frames** (sometimes also called Giants) are Ethernet frames with more than **1518 bytes** (MTU-Size, 18 Bytes overhead) of payload. Conventionally, jumbo frames can carry up to **9216 bytes** of payload, but variations exist and some care must be taken using the term. Many Gigabit Ethernet switches and Gigabit Ethernet network interface cards support jumbo frames. Some Fast Ethernet switches and Fast Ethernet network interface cards also support jumbo frames. Most

national research and education networks (such as Internet2, National LambdaRail, ESnet, GÉANT and AARNet) support jumbo frames, but most commercial Internet service providers do not.

Source: Wikipedia

- Jumbo Frames should not be confused with **jumbograms**.
- The end-to-end MTU size depends on the devices on the way.
If not all devices support Jumbo Frames, you will face "**Jabber**"
- To investigate the possible frame sizes, use "**Path MTU Discovery**"

Windows:

nca.cpl

Local Area Connection Properties

Configure → Advanced → Jumbo Packet: Enable: 9014 Bytes

Configure Cisco IOS devices:

```
Router(config)# interface GigabitEthernet 4/1
```

```
Router(config-if)# mtu 9216
```

Check MTU size: show interface



Koppelnetz / Coupling Network

The point of proper IP address design is that you don't use any more IP addresses than are absolutely needed. With a /30 bit subnet mask providing us 2 useable IP addresses, let's think of a network where there are only 2 hosts. While this idea seems silly for IP Addressing on a LAN, it is actually perfect for IP addressing on **WAN connections** or any **router to router connections**.

For example, say that I get an **Internet T1 circuit**. I setup my router and connect to the ISP's router. An @Internet circuit is treated like a **point to point WAN circuit**. There are only 2 routers on that circuit, each connecting to each other (coupling). Then you need a **network address** so that that entire network can be represented in a routing table. I really don't see any purpose for the broadcast in that scenario but if you have a network then you also have a broadcast.

The /30 subnet mask provides the most efficient use of IP addresses by not wasting any IP addresses when it is applied to a **point to point network connection**.

So what is a /30 bit mask? A /30 bit mask would be 30 one's, leaving just 2 zero's that could be used for host addressing. If you apply the hosts formula, you get $2^2 = 4 - 2 = 2$ useable IP addresses. In other words, our network would look like this:

- Network address
- Host IP
- Host IP
- Broadcast

Layer 2 VPN

tbd

Layer 3 VPN

IPSec

Lightweight Third-Party Authentication (LTPA)

Is an authentication technology used in **IBM WebSphere** and **Lotus Domino** products. When accessing web servers that use the LTPA technology it is possible for a web user to re-use their login across physical servers.

A Lotus Domino server or an IBM WebSphere server that is configured to use the LTPA authentication will challenge the web user for a name and password. When the user has been authenticated, their browser will have received a **session cookie** - a cookie that is only available for one browsing session. This cookie contains the LTPA token.

If the user - after having received the LTPA token - accesses a server that is a member of the same authentication configuration as the first server, and if the browsing session has not been terminated (the browser was not closed down), then the user is automatically authenticated and will not be challenged for a name and password. Such an environment is also called a **Single-Sign-On (SSO)** environment.

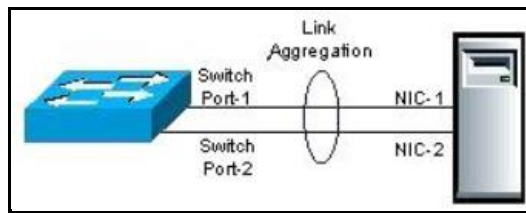
Source: Wikipedia

Link Aggregation Control Protocol (LACP)

Link aggregation is a computer networking term to describe various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain, and to provide redundancy in case one of the links fail.

See also: IEEE 802.1ax or IEEE 802.3ad

Source: Wikipedia



Metro Ethernet Forum (MEF)

The **Metro Ethernet Forum (MEF)**, founded in 2001, is a nonprofit international industry consortium, dedicated to worldwide adoption of Carrier Ethernet networks and services.

Source: Wikipedia

Maximum Transmission Unit (MTU)

See RFC 791, 1122

- A common value on a router is **1500 bytes** MTU.
- Frames that barely exceed the MTU size are called "**baby giant frames**" or **oversize frames**.
- **802.3ac** extends the maximum frame length to **1522 bytes**.

Find out Path MTU

```
ping <IP-Address> -a -f -l 1472
```

```
ping <IP-Address> -a -f -l 1450
```

PMTU - SAP

PMTU

Medium	MTU in Bytes
Hyperchannel	65535
Token Ring(4)(802.5)	4464
Token Ring(16)	17914
FDDI	4352
Ethernet	1500
Gigabit Ethernet mit Jumboframes	9000
PPPoE (z. B. DSL)	≤ 1492
SLIP/PPP (low delay)	296
X.25	576
FibreChannel	theoretisch unbegrenzt
ISDN	576
DQDB	
HIPPI	
ATM	4500, s. u.
ARCNET	
802.11	2312 (WiFi)

Figure 99: Typical MTU-Sizes

Multiprotocol Label Switching (MPLS)

Layer 3

Nagles's Algorithm

RFC 896, 1122

Nagle's algorithm, named after John Nagle, is a means of improving the efficiency of TCP/IP networks by **reducing the number of packets that need to be sent over the network**.

Nagle's document, Congestion Control in IP/TCP Internetworks (RFC 896) describes what he called the "**small packet problem**", where an application repeatedly emits data in small chunks, frequently only 1 byte in size. Since TCP packets have a 40 byte header (20 bytes for TCP, 20 bytes for IPv4), this results in a 41 byte packet for 1 byte of useful information, a huge overhead. This situation often occurs in Telnet sessions, where most keypresses generate a single byte of data that is transmitted immediately. Worse, over slow links, many such packets can be in transit at the same time, potentially leading to congestion collapse.

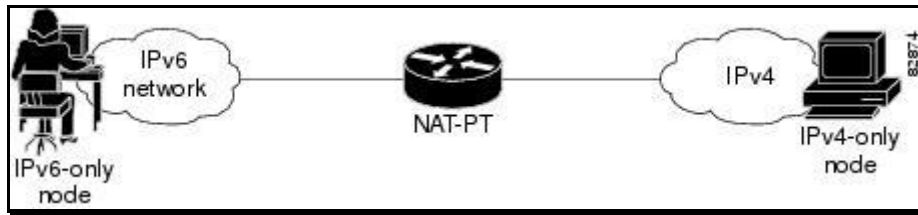
Nagle's algorithm works by combining a number of small outgoing messages, and sending them all at once. Specifically, as long as there is a sent packet for which the sender has received no acknowledgment, the sender should keep buffering its output until it has a full packet's worth of output, so that output can be sent all at once.

TCP_NODELAY Standard = enabled

This may influence interactive applications negative (Latency)

NAT-PT for IPv6

- **Network Address Translation-Port Translation** (NAT-PT) for Cisco software based on RFC 2766 and RFC 2765 is a migration tool that helps customers transition their IPv4 networks to IPv6 networks. Using a protocol translator between IPv6 and IPv4 allows direct communication between hosts that use different network protocols. You can use **static** or **dynamic**, port address translation, IPv4-mapped definitions for NAT-PT operation.
- The figure below shows that NAT-PT runs on a device that is configured between an IPv6 network and an IPv4 network that helps connect an IPv6-only node with an IPv4-only node.



- NAT-PT allows direct communication between **IPv6-only** networks and **IPv4-only** networks. Dual-stack networks (networks that have IPv4 and IPv6) can have some IPv6-only hosts configured to take advantage of the IPv6 autoconfiguration, global addressing, and simpler management features, and these hosts can use NAT-PT to communicate with existing IPv4-only networks in the same organization.
- One of the benefits of NAT-PT is that no changes are required to existing hosts if NAT-PT is configured, because all NAT-PT configurations are performed at the NAT-PT device. Stable IPv4 networks can introduce an IPv6 network and use NAT-PT to communicate between these networks without disrupting the network. For a seamless transition, you can use **FTP** between IPv4 and IPv6 hosts.
- When you configure IPv6, packet fragmentation is enabled by default, to allow IPv4 and IPv6 networks to resolve fragmentation problems. Without the ability to resolve fragmentation, connectivity can be intermittent when fragmented packets are dropped or not interpreted correctly.
- We do not recommend the use of NAT-PT to communicate between a dual-stack host and an IPv6-only or IPv4-only host.
- We do not recommend the use of NAT-PT in a scenario in which an IPv6-only network tries to communicate with another IPv6-only network via an IPv4 backbone or vice versa, because NAT-PT requires a **double translation**. You can use tunneling techniques for communication in these scenarios.
- You can configure one the following operations for NAT-PT, but not all four.
- NAT-PT is not supported in **Cisco Express Forwarding (CEF)** and must be disabled.

NetBIOS over TCP/IP (NBT, NetBT)

RFC 1001, 1002

Performs computer name to IP address mapping, name resolution (NETBT.SYS in Windows NT and VNBT.VXD in Windows for Workgroups and Windows 95). There are currently four NetBIOS over TCP/IP name resolution methods: **b-node**, **p-node**, **m-node** and **h-node**.

Port 137_udp	NetBIOS Name resolution
Port 138_udp	Datagram Service
Port 139_tcp	Session Service

Older Windows Systems like WfW, Windows 95, Windows NT & Windows 2000 are using this for:

- Server Message Block (SMB)
New windows systems are using Port 445_tcp for this.
- Windows 2000 workstation service
- Server service
- Computer-Browser (Computersuchdienst)
 - Domain Master Browser
 - Backup Browser
 - Master Browser
 - See Service <browser>

```
sc stop browser
sc config browser start=disabled
```
 - Registry Keys:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Browser\Parameters
MaintainServerList = Yes/Auto
IsDomainMasterBrowser = yes
```
- Messenger
- NetLogon services
- net use x:\<fqdn>\data
- net use x:\<IP>\data

- net view
- net send
- dir \\<fqdn>\data

Howto disable NetBIOS over TCP/IP (NBT) support:

1. ncpa.cpl
2. Select Local Area Connection and right-click Properties
3. Select Internet Protocol Version 4 (TCP/IPv4), click on Properties button.
4. Select WINS
5. Click Disable NetBIOS over TCP/IP

Unique NetBIOS Names Used by Microsoft Components

Unique Name	Service
<computer_name>[00] (space filled)1	Workstation Service
<computer_name>[03] (space filled)	Messenger Service
<computer_name>[06] (space filled)	RAS Server Service
<computer_name>[1F] (space filled)	NetDDE Service
<computer_name>[20] (space filled)	Server Service
<computer_name>[21] (space filled)	RAS Client Service
<computer_name>[BE] (0xBE filled)	Network Monitor Agent
<computer_name>[BF] (0xBF filled)	Network Monitor Application
<user_name>[03] (space filled)	Messenger Service
<domain_name>[1D] (space filled)	Master Browser
<domain_name>[1B] (space filled)	Domain Master Browser

1 The number in brackets is a hexadecimal number. (space filled) means that if the computer or domain name is not 15 characters long, the name is filled with spaces up to 15 characters.

Group NetBIOS Names Used by Microsoft Components

Group Name	Service
<domain_name>[00] (space filled)	Domain Name
<domain_name>[1C] (space filled)	Domain Controllers
<domain_name>[1E] (space filled)	Browser Service Elections
[01h][01h]__MSBROWSE__[01h][01h]	Master Browser

Network Address Translation (NAT)

Is a methodology of remapping one IP address space into another by modifying network address information in Internet Protocol (IP) datagram packet headers while they are in transit across a traffic routing device. The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host. It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion.

See also DNS64.

Source: Wikipedia

Network Address Translation 64 (NAT64)

- Translation of **IPv4 addresses** in **IPv6 Addresses** and vice versa. Main purpose to allow **pure IPv6 Networks to access IPv4 hosts**.
- Uses the reserved address space **2002::/16**.
e.g. **2002:router-IPv4-address::/48**
- Used if you plan to migrate to IPv6 and you will use the **dual-stack** approach.
- **Stateful NAT64 (1:N)** uses a single IP address with different port numbers for all the private users.
- **Stateless NAT64 (1:1)** you need for every IPv6 address a IPv4 address.
- **Manually** configured NAT64 tables are called **stateless**.
- NAT64 is usually implemented in conjunction with **DNS64**.
- You may setup **NAT64** over **NAT-PT**.
- NAT64 modifies **sessions** during translation.
- NAT64 uses **network specific prefixes** assigned by an organization.
- Uses **Well-Known Prefix (WKP)**.
- Supports **application layer gateway**.

Well-Known prefix (WKP): **64:ff9b::/96**

- Used for **Stateful** IPv4/IPv6 translation service (NAT64)

- **Googles DNS64 Prefix**
- See RFC 6052, 3848-revise (NAT64)

Stateless NAT64	Stateful NAT64
1:1 translation	1:N translation
No conservation of IPv4 address	Conserves IPv4 address
Assures end-to-end address transparency and scalability	Uses address overloading, hence lacks in end-to-end address transparency
No state or bindings created on the translation	State or bindings are created on every unique translation
Requires IPv4-translatable IPv6 addresses assignment (mandatory requirement)	No requirement on the nature of IPv6 address assignment
Requires either manual or DHCPv6 based address assignment for IPv6 hosts	Free to choose any mode of IPv6 address assignment with Manual, DHCPv6, SLAAC

Network Prefix Translation version 6 (NPTv6)

- Simply translates **one IPv6** prefix to another (**1:1**) and cannot be **overloaded**.
- Sometimes referred as **IPv6-to-IPv6 Network**.
- It is **checksum-neutral**.
- A major benefit associated with NPTv6 is the fact that it avoids the requirement for an **NPTv6 Translator** to rewrite the **transport layer headers** which reduces the load on network devices.
- Does **not** rewrite **higher layer** informations.
- NPTv6 is **stateless**.
- Sometimes called **NAT66**.
- For internal devices the range **FC00::/7** can be used.

Network Device Enrollment Service (NDES)

The Network Device Enrollment Service (NDES) is one of the role services of the Active Directory Certificate Services (AD CS) role. It implements the Simple Certificate Enrollment Protocol (SCEP). SCEP defines the communication between network devices and a Registration Authority (RA) for certificate enrollment and is defined in detail in:

<http://tools.ietf.org/html/draft-nourse-scep-18>

"The goal of SCEP is to support the secure issuance of certificates to network devices in a scalable manner, using existing technology whenever possible."

Warning:

SCEP was designed to be used in a closed network where all end-points are trusted. The warnings from CERT in the article "Simple Certificate Enrollment Protocol (SCEP) does not strongly authenticate certificate requests " should be considered when implementing the NDES service. If an application utilizes SCEP, it should provide its own strong authentication.

Source: Microsoft TechNet

Network Policy Server (NPS)

Network Policy and Access Services (NPAS)

- Is a component of Windows Server 2008. It replaces the Internet Authentication Service (IAS) from Windows Server 2003.
- It authenticates and authorizes the connection request before allowing or denying access.

Possible Authentication Methods:

- Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP)
Requires: <username> and <password> verifies the credentials against the user accounts database.
Security wise not recommended!
- Certificate-based credentials
Strong security

Network TAP

A **network tap** is a hardware device which provides a way to access the data flowing across a computer network. In many cases, it is desirable for a third party to monitor the traffic between two points in the network. If the network between points A and B consists of a physical cable, a "network tap" may be the best way to accomplish this monitoring. The network tap has (at least) three ports: an **A** port, a **B** port, and a **monitor** port. A tap inserted between A and B passes all traffic through unimpeded, but also copies that same data to its monitor port, enabling a third party to listen.

Source: Wikipedia

Network Test Access Point more commonly known as TAP is a device that enable network and security personnel to access data passing through the network for monitoring and analysis purposes. Taps are passive devices. Most taps pass all seven layers of OSI network traffic (including layer 1 and layer 2 errors) and do not interfere with the performance of the network or the data stream of the network traffic.

Network News Transfer Protocol (NNTP)

- **Network News Transfer Protocol (NNTP)** is the Internet news protocol for the distribution, inquiry, retrieval, and posting of news articles.
- **USENET**, the Internet news service, provides bulletin boards, chat rooms (real-time chat sessions), and access to newsgroups. Only group members can participate in a newsgroup. Newsgroups can be excellent sources of technical information and forums for information interchange.

Payload

- **Payload** in computing (sometimes referred to as the actual or body data) is the cargo of a data transmission.
- It is the part of the transmitted data, which is the fundamental purpose of the transmission, to the exclusion of information sent with it (such as headers or metadata, sometimes referred to as overhead data) solely to facilitate delivery.

PIP

- ???

PKCS

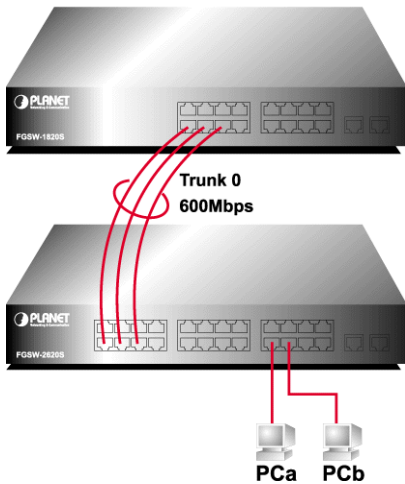
- In cryptography, **PKCS** is a group of **public-key cryptography standards** devised and published by RSA Security Inc, starting in the early 1990s.
- The company published the standards to promote the use of the cryptography techniques to which they had patents, such as the **RSA** algorithm, the Schnorr signature algorithm and several others.

Source: Wikipedia

Preferred: **PKCS#7**

Port Trunking

About Port Trunking



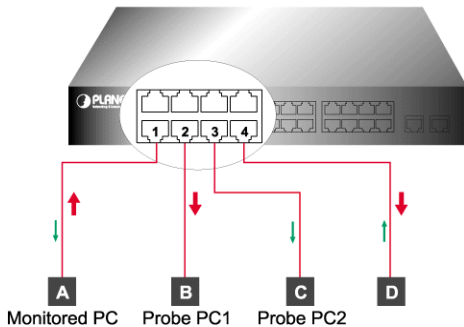
In the past, to increase your port density, there is two alternatives, stack the device, or cascade the device using the front-end port with only one link. For the first, the back plane is much bigger, yet it won't take any ports from you, however, you also could get the budget consideration. As for the second, the cost is ok, but the only problem is the bandwidth bottleneck.

And now, to solve the bottleneck, the Smart Switch use the port-trunk technology that help to increase the path between two devices, double, fourfold the bandwidth, or more. Determining how many bandwidths are required for your networks, enabling the ports and make the connection with just plug-in. No needs of any skill but just wire connection.

The Smart Switch support flexibility of wiring, up to 2 links for Gigabit ports having 4Gbps (full-duplex) bandwidth, and 4 links (800Mbps) for Fast Ethernet ports, yet, FGSW family supports up to 8 links, i.e.

1.6Gbps (full-duplex) bandwidth. Increase the bandwidth on demand.

About Port Mirroring



To monitor the network performance and diagnose the network problem should an easy job in a hub. But, not for a switch, just because that, it is not a sharing device.

However, with port mirroring, now the network manager can watch any port as wish due to the Smart Switch duplicate the packets to you. It is simple to see what's going on in your switched network domain without disturbing that.

Proxy Automatic Config (PAC)

PROXY.PAC

Rack - Mounted Automatic Transfer Switch (ATS)

Rack Automatic Transfer Switches (rack ATS) provide reliable, redundant rack mount power to single-corded equipment. The rack ATS has dual input power cords supplying power to the connected load. If the primary power source becomes unavailable, the rack ATS will seamlessly source power from the secondary source without interrupting critical loads. The Rack ATS has built-in network connectivity, which allows for remote management via Web, SNMP, or Telnet interfaces.

RARP - Reverse Address Resolution Protocol

- RARP is used to resolve MAC addresses into IP addresses.

RIPE Network Coordination Centre (NCC)

<http://www.ripe.net>

- RIPE maintains a database (WHOIS) of all registered IP address blocks and information about who is using this address space in Europe and the Middle-East.
- When an ISP allocates address space to another company, it registers this allocation by sending an RIPE report to Whois.

Routing Information Protocol (RIP)

- Is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric.
- RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.
- The maximum number of hops allowed for RIP is 15.
- This hop limit, however, also limits the size of networks that RIP can support.
- A hop count of 16 is considered an infinite distance, in other words the route is considered unreachable.

Source: Wikipedia

RTP - Real Time Transport Protocol

- RTP packets have the same characteristics as VoIP packets.

The **Real-time Transport Protocol (RTP)** is a network protocol for delivering audio and video over IP networks. RTP is used extensively in communication and entertainment systems that involve streaming media, such as telephony, video teleconference applications, television services and web-based push-to-talk features.

RTP typically runs over **User Datagram Protocol (UDP)**. RTP is used in conjunction with the RTP Control Protocol (RTCP). While RTP carries the media streams (e.g., audio and video), RTCP is used to monitor transmission statistics and **quality of service (QoS)** and aids synchronization of multiple streams. RTP is one of the technical foundations of **Voice over IP** and in this context, is often used in conjunction with a signaling protocol such as the **Session Initiation Protocol (SIP)** which establishes connections across the network.

RTP was developed by the Audio-Video Transport Working Group of the Internet Engineering Task Force (IETF) and first published in 1996 as RFC 1889, superseded by RFC 3550 in 2003.

Source: Wikipedia

Simple Certificate Enrollment Protocol (SCEP)

Simple Certificate Enrollment Protocol is an Internet Draft in the Internet Engineering Task Force (IETF). This protocol is being referenced by several manufacturers of network equipment and software who are developing simplified means of handling certificates for large-scale implementation to everyday users.

The protocol is designed to make the **issuing** and **revocation** of digital certificates as scalable as possible. The idea is that any standard network user should be able to request their digital certificate electronically and as simply as possible. These processes have usually required intensive input from network administrators, and so have not been suited to large scale deployments.

SCEP is the most popular, widely available and most tested certificate enrollment protocol. It has several advantages over competing protocols, such as Certificate Management Protocol.

Source: Wikipedia

Small form-factor pluggable transceiver (SFP)

The **small form-factor pluggable (SFP)** is a compact, hot-pluggable transceiver used for both telecommunication and data communications applications. The form factor and electrical interface are specified by a multi-source agreement (MSA). It interfaces a network device motherboard (for a switch, router, media converter or similar device) to a fiber optic or copper networking cable. It is a popular industry format jointly developed and supported by many network component vendors. SFP transceivers are designed to support SONET, Gigabit Ethernet, Fibre Channel, and other communications standards. Due to its smaller size, SFP obsolesces the formerly ubiquitous gigabit interface converter (GBIC); the SFP is sometimes referred to as a **Mini-GBIC** although no device with this name has ever been defined in the MSAs.



Figure 100: SFP

Types

SFP transceivers are available with a variety of transmitter and receiver types, allowing users to select the appropriate transceiver for each link to provide the required *optical reach* over the available optical fiber type (e.g. multi-mode fiber or single-mode fiber). Optical SFP modules are commonly available in several different categories:

for multi-mode fiber, with black or beige extraction lever

SX - 850 nm, for a maximum of 550 m at 1.25 Gbit/s (Gigabit Ethernet) or 150m at 4.25 Gbit/s (Fibre Channel)

for single-mode fiber, with blue extraction lever

LX - 1310 nm, for distances up to 10 km

EX - 1310 nm, for distances up to 40 km

ZX - 1550 nm, for distances up to 80 km

EZX - 1550 nm, for distances up to 120 km

BX - 1490 nm/1310 nm, Single Fiber Bi-Directional Gigabit SFP Transceivers, paired as **BS-U** and **BS-D** for Uplink and Downlink respectively, also for distances up to 10 km. Variations of bidirectional SFPs are also manufactured which use 1550 nm in one direction.

1550 nm 40 km (**XD**), 80 km (**ZX**), 120 km (**EX** or **EZX**)

SFSW - Single Fiber Single Wavelength transceivers, for bi-directional traffic on a single fiber.

Coupled with CWDM, these double the traffic density of fiber links.

CWDM and DWDM transceivers at various wavelengths achieving various maximum distances for copper twisted pair cabling

1000BASE-T - these modules incorporate significant interface circuitry-and can only be used for Gigabit Ethernet, as that is the interface they implement. They are not compatible with (or rather: do not have equivalents for) Fibre channel or SONET.

Source: Wikipedia

Software as a Service (SaaS)

Software as a service, or "Service(s) as a Software Substitute" (SaaS), is a software licensing and delivery model in which software is licensed on a subscription basis and is centrally hosted on the cloud by independent software vendors (ISVs) or application service providers (ASPs). It is sometimes referred to as "service(s) as a software substitute" (SaaS) or "on-demand software". SaaS is typically accessed by users using a thin client via a web browser. SaaS has become a common delivery model for many business applications, including office & messaging software, DBMS software, management software, CAD software, dDevelopment software, gamification, virtualization, accounting, collaboration, customer relationship management (CRM), management information systems (MIS), enterprise resource planning (ERP), invoicing, human resource management (HRM), content management (CM) and service desk management. SaaS has been incorporated into the strategy of all leading enterprise software companies. One of the biggest selling points for these companies is the potential to reduce IT support costs by outsourcing hardware and software maintenance and support to the SaaS provider.

According to a Gartner Group estimate, SaaS sales in 2010 reached \$10 billion, and were projected to increase to \$12.1bn in 2011, up 20.7% from 2010. Gartner Group estimates that SaaS revenue will be more than double its 2010 numbers by 2015 and reach a projected \$21.3bn. Customer relationship management (CRM) continues to be the largest market for SaaS. SaaS revenue within the CRM market was forecast to reach \$3.8bn in 2011, up from \$3.2bn in 2010.

The term "software as a service" (SaaS) is considered to be part of the nomenclature of cloud computing, along with **infrastructure as a service (IaaS)**, **platform as a service (PaaS)**, **desktop as a service (DaaS)**, **backend as a service (BaaS)**, and **information technology management as a service (ITMaas)**.

Source: Wikipedia

Examples: online word processing and spreadsheet tools, CRM services and web content delivery services (e.g. Salesforce CRM, Microsoft Office 365, Google Docs, etc.).

Cisco Cloud Web Security (prev. ScanSafe)

Sprint solution: Cisco Cloud Web Security / SaaS

See: <http://www.cisco.com/c/en/us/products/security/cloud-web-security/index.html>

Spanning Tree Protocol (STP, IEEE 802.1D)

The **Spanning Tree Protocol (STP)** is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Source: Wikipedia

Split tunneling

Is a computer networking concept which allows a VPN user to access a public network (e.g., the Internet) and a local LAN or WAN at the same time, using the same physical network connection. This connection service is usually facilitated through a program such as a VPN client software application. For example, suppose a user utilizes a remote access VPN software client connecting to a corporate network using a hotel wireless network. The user with split tunneling enabled is able to connect to file servers, database servers, mail servers and other servers on the corporate network through the VPN connection. When the user connects to Internet resources (Web sites, FTP sites, etc.), the connection request goes directly out the gateway provided by the hotel network.

Advantages

One advantage of using split tunneling is that it alleviates bottlenecks and conserves bandwidth as Internet traffic does not have to pass through the VPN server.

Another advantage is in the case where a user works at a supplier or partner site and needs access to network resources on both networks throughout the day. Split tunneling prevents the user from having to continually connect and disconnect.

Disadvantages

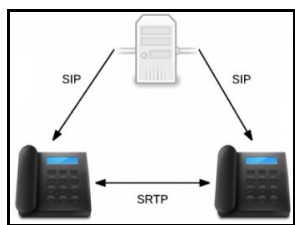
A disadvantage is that when split tunneling is enabled, users bypass gateway level security that might be in place within the company infrastructure. For example, if web or content filtering is in place, this is something usually controlled at a gateway level, not the client PC.

ISPs that implement DNS hijacking break name resolution of private addresses with a split tunnel.

Source: Wikipedia

SRTP - Secure Real Time Transport Protocol

- Ist ein Erweiterungsprofil des RTP (Real-Time Transport Protocol).
- SRTP fügt zusätzliche Sicherheitsfunktionalitäten hinzu, darunter Authentifizierung von Nachrichten, Vertraulichkeitsschutz und Wiedergabeschutz, welche bei der Kommunikation per VoIP eine wesentliche Rolle spielen.
- SRTP nutzt Authentifizierungs- und Verschlüsselungsmethoden, um das Risiko von Angriffen wie Denial of Service weitmöglichst zu minimieren.
- Das Protokoll wurde 2004 durch die IETF (Internet Engineering Task Force) als RFC 3711 veröffentlicht. SRTP, wie auch DTLS ist eines der sichersten Protokolle, welche der WebRTC-Technologie zur Verfügung stehen



Synchronous Optical Networking (SONET)

Synchronous Optical Networking (SONET) and Synchronous Digital Hierarchy (SDH) are standardized protocols that transfer multiple digital bit streams over optical fiber using lasers or highly coherent light from light-emitting diodes (LEDs).

Source: Wikipedia

Symmetric Digital Subscriber Line (SDSL)

Internet access technologies based on **DSL** that offer symmetric bandwidth upstream and downstream. It is considered the opposite of asymmetric digital subscriber line (**ADSL**) technologies where the upstream bandwidth is lower than the downstream bandwidth.

Source: Wikipedia

Server Hosting

Providing the HW for a customer server.

Server Housing

Providing network connection and space for a customer server.

Server Message Block (SMB 3.0)

- Also known as **Common Internet File System (CIFS)**.
- SMB 1.0
- The **SMB 2.x** protocol was introduced in **Windows Server 2008** and in **Windows Vista**.
- The **SMB 3.0** protocol was introduced in **Windows Server 2012** and in **Windows 8**.
-

The Server Message Block (SMB) Protocol Versions **2** and **3** supports the sharing of file and print resources between machines.

New SMB features:

- SMB Transparent Failover
- SMB Scale Out
- SMB Multichannel
- SMB Direct
- SMB Encryption
- VSS for SMB file shares
- SMB Directory Leasing
- SMB PowerShell

Switched Port Analyzer (SPAN)

Technique: Port mirroring.

Sends a copy of the traffic of one port to another port for monitoring, IDS etc.

Configuring SPAN

```
(config)#monitor session 1 source interface fa0/1
```

```
(config)#monitor session 1 dest interface fa0/2
```

```
#show monitor
```

Remote Catalyst Switched Port Analyzer (RSPAN)

Technique: Port mirroring.
Sends a copy of the traffic of one port to another port for monitoring, IDS etc. by encapsulating the copied traffic into a VLAN and forward the traffic to another switch.

- RSPAN allows you to monitor traffic if the source and destination ports are not located on the same switch.

Configuring RSPAN

```
(config)#monitor session 1 source interface fa0/1  
(config)#monitor session 1 dest interface fa0/2
```

```
#show monitor
```

SMTP

- Is **part of the TCP/IP** protocol suite. It defines the protocol that sends and receives e-mail messages.
- Provides an address book feature and the handshaking specifications for connection verification, message transmission, transmission parameters, and user identification.
- **MHS** (Message Handling Service) is a defacto standard, similar to X.400, that has been popularized by Novell

Split-Brain

High-availability clusters usually use a **heartbeat private network** connection which is used to monitor the health and status of each node in the cluster. For example the **split-brain syndrome** may occur when **all** of the private links **go down simultaneously**, but the cluster nodes are still running, each one believing they are the only one running. The data sets of each cluster may then randomly serve clients by their own "idiosyncratic" data set updates, without any coordination with the other data sets.

SMLT - Split Multi Link Trunk

Split Multi-Link Trunking (SMLT) is a Layer 2 link aggregation technology in computer networking originally developed by Nortel as an enhancement to standard multi-link trunking (MLT) as defined in IEEE 802.3ad.

Link aggregation or **MLT** allows multiple physical network links between two network switches and another device (which could be another switch or a network device such as a server) to be treated as a single logical link and load balance the traffic across all available links. For each packet that needs to be transmitted, one of the physical links is selected based on a load-balancing algorithm (usually involving a hash function operating on the source and destination Media Access Control (MAC) address information). For real-world network traffic this generally results in an effective bandwidth for the logical link equal to the sum of the bandwidth of the individual physical links. Redundant links that were once unused due to Spanning Tree's loop protection can now be used to their full potential.

A general limitation of standard link aggregation, **MLT** or EtherChannel is that all the physical ports in the link aggregation group must reside on the same switch. The SMLT, DSMLT and RSMLT protocols remove this limitation by allowing the physical ports to be split between two switches, allowing for the creation of Active load sharing high availability network designs that meet five nines availability requirements.

Source: Wikipedia

Squid

Squid is a **caching** and **forwarding web proxy**. It has a wide variety of uses, from speeding up a web server by caching repeated requests; to caching web, DNS and other computer network lookups for a group of people sharing network resources; to aiding security by filtering traffic. Although primarily used for **HTTP** and **FTP**, Squid includes limited support for several other protocols including **TLS**, **SSL**, **Internet Gopher** and **HTTPS**.

Squid was originally designed to run as a daemon on Unix-like systems. A Windows port was maintained up to version 2.7, but more current versions are not being developed. Squid is free software released under the **GNU** General Public License.

Source: Wikipedia

SSLvX

- SSLv2 Is insecure and shouldn't be used.
- SSLv3 Is insecure and should be disabled (see POODLE)

Switching

Layer 1

Switching on physical level (Hubs, Repeater)

Layer 2

Switching on MAC-Address level (Switch)

- Store and Forward Technology (Slow)
- Cut-Through-Forwarding Technology (Fast)

Layer 3

Switches on IP-Address level (Router & Switch)

- Routing functions for VLAN's

- Supports: RIP / RIP2 / OSPF

Layer 4

Switching on IP-Address level + Ports

- Frontend for Webserver-Cluster, allows load balancing.
- Webserver must be identical (replicated)

Layer 5

- Frontend for Webserver-Cluster, allows load balancing.
- Webserver must not be identical websites kann be distributed on different servers.
- Can switch based on URL's

Layer 7

Switches on Uniform Resource Locator (URL) level.

Tail-Drop

- Term for Switches and Routers to describe full queue congestion results in the dropping of all packets at the tail end of the queue (tail drop).

Can cause:

- TCP starvation
- Global synchronization

TCP/IP Stack (OSI & TCP-Model)

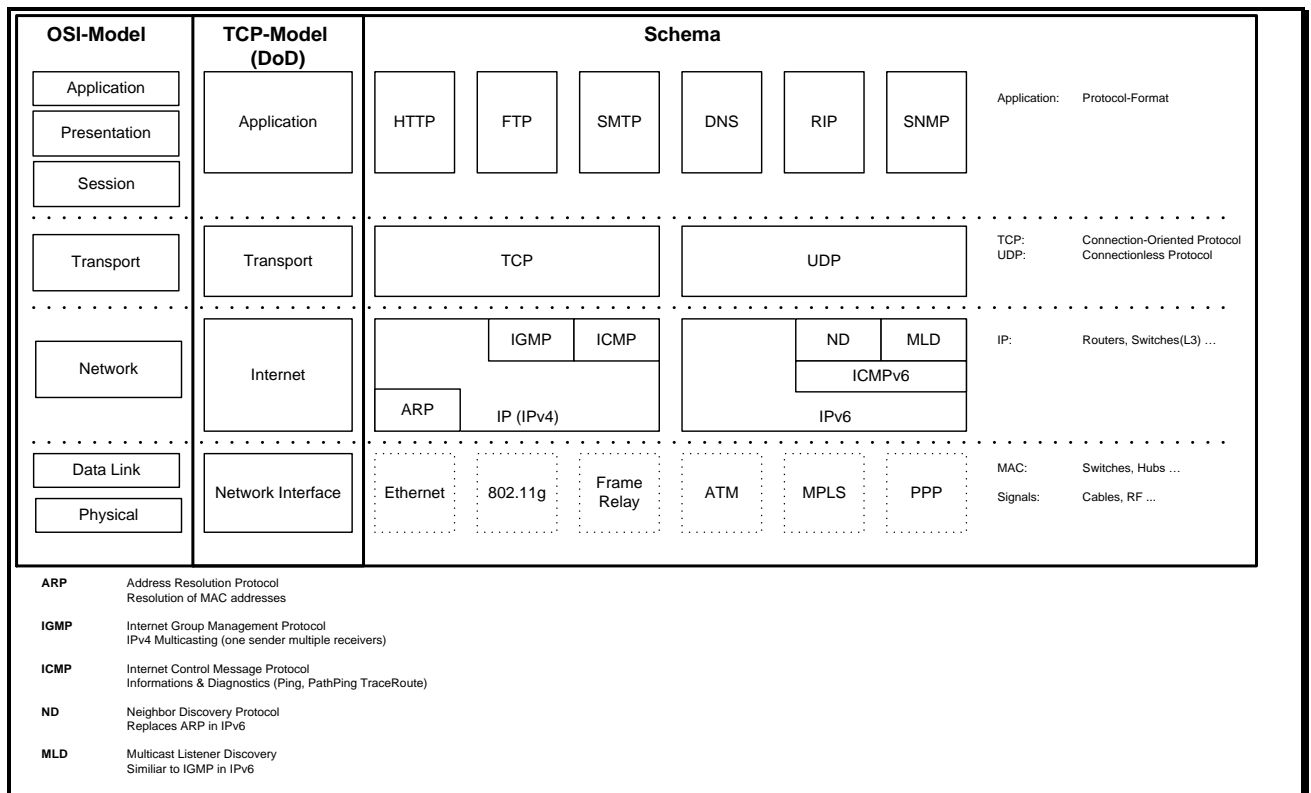


Figure 101: TCP/IP Stack

Telnet

- Telnet is terminal emulation software used to connect an Internet client to a host.
- Once connected, the client can access host files as if it were locally connected.

Teredo

RFC 4380

In computer networking, **Teredo** is a transition technology that gives full IPv6 connectivity for IPv6-capable hosts which are on the IPv4 Internet but which have no direct native connection to an IPv6 network. Compared to other similar protocols its distinguishing feature is that it is able to perform its function even from behind network address translation (NAT) devices such as home routers. Teredo operates using a platform independent tunneling protocol designed to **provide IPv6 (Internet Protocol version 6) connectivity by encapsulating IPv6 datagram packets within IPv4 User Datagram Protocol (UDP) packets**. These datagrams can be routed on the IPv4 Internet and through NAT devices. Other Teredo nodes elsewhere called **Teredo relays** that have access to the IPv6 network then receive the packets, unencapsulate them, and route them on. Teredo is designed as a last resort transition technology and is intended to be a temporary measure: in the long term, all IPv6 hosts should use native IPv6 connectivity. Teredo should therefore be disabled when native IPv6 connectivity becomes available. Teredo was developed by Christian Huitema at Microsoft, and was standardized in the IETF as RFC 4380. The Teredo server listens on UDP port 3544.

Source: Wikipedia

Check Teredo

See: Communication General.docx

Deaktiviere Teredo

See: Communication General.docx

Time Zones / Zeitzone

UTC	Coordinates Universal Time	
CET	Central European Time	
CEST	Central European Summer Time	
MEZ	Mitteleuropäische Zeit	UTC+1
MESZ	Mitteleuropäische Sommerzeit	UTC+2
EST	Eastern Standard Time	
GMT	Greenwich mean time	

TINA VPN Tunnel

Proprietary IPsec Protocol for "Barracuda" FW Systems:

You can use the **TINA** protocol for VPN connections between two Barracuda NG Firewalls whereas **IPsec** is only used for VPN tunnels between a Barracuda NG Firewall gateway and a system of a different manufacturer.

Trusted Platform Module (TPM)

Acts like a smartcard in the computer and builds a so called "Trusted Computer Platform". Identifies secure a computer, based on a certificate.

Transport Layer Security (TLS)

- **TLS 1.0** Common used, still secure
- **TLS 1.1** Without known security issues
- **TLS 1.2** Without known security issues, seldom used

TLS/SSL is super simple to install and deploy on your server. If you do not set it up correctly, you're not going to protect your data and may run into problems.

Universal Mobile Telecommunications System (UMTS)

Is a third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology. UMTS uses wideband code division multiple access (W-CDMA) radio access technology to offer greater spectral efficiency and bandwidth to mobile network operators.

Source: Wikipedia

Variable-Length Subnet Masking (VLSM)

To divide the entire network into only one level of subnetworks doesn't represent the best use of our IP address block.

10.0.0.0/8 Single Subnet

VLSM

10.0.0.0/8 Single Subnet

10.x.x.0/24 Subnet 1

10.x.x.0/26 Subnet 2

...

Only classes Routing-Protocols can support VLSM, such as OSPF, EIGRP

Very-high-bit-rate Digital Subscriber Line (VDSL or VHDSL)

Is a digital subscriber line (DSL) technology providing data transmission faster than ADSL over a single flat untwisted or twisted pair of copper wires (up to 52 Mbit/s downstream and 16 Mbit/s upstream), and on coaxial cable (up to 85 Mbit/s down- and upstream); using the frequency band from 25 kHz to 12 MHz. These rates mean that VDSL is capable of supporting applications such as high-definition television, as well as telephone services (voice over IP) and general Internet access, over a single connection. VDSL is deployed over existing wiring used for analog telephone service and lower-speed DSL connections. This standard was approved by ITU in November 2001. GPRS

Source: Wikipedia

Virtual LAN (VLAN)

A VLAN is a logical grouping of network devices put together as a LAN regardless of their physical grouping or collision domains. VLANs let a user see and access only specified network segments. This optimizes network efficiency and maintains security access restrictions. VLANs require **special switches** that are capable of supporting VLANs.

A VLAN offers you the ability to group users and client PCs together into logical workgroups, a critical consideration when connecting clients to servers that are geographically dispersed across the building, campus, or enterprise network.

Typically, VLANs consist of a common set of coworkers within the same department but in different locations, a cross-functional team working on a joint project, or a diverse set of users sharing the same network application. Joining workers across the network forms logical working groups.

By using VLANs on your network, you can:

- Improve network performance
- Limit broadcast storms
- Improve adds, moves, and changes
- Minimize security problems
- Ease your management task

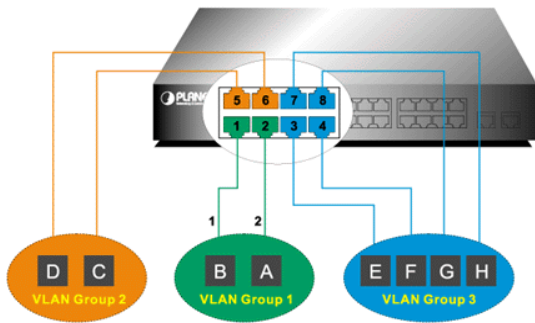
For overview information on Intel VLANs, visit the Intel Networking Web site:

<http://www.intel.com/network>

For more specific information, read the white paper on VLANs:

http://www.intel.com/network/tech_brief/virtual_lans.htm

[About VLAN](#)



The VLAN (Virtual LAN) is a method to separate different Networks in one Switch. For example, there is two workgroups (A/B) connect to the Switch. Without any setting of VLAN or with a standard switch, it is easy to make the connection between A and B. That's also means, every broadcast from A will also being heard by B.. This cause two issues, in logical, the security issue and in physical, the performance issue. i.e. A don't need to see B. And B does not need to receive the useless broadcast packets from A that could effects the bandwidth and performance.

The Smart Switch can easily separate A and B by ports. A and B will never see each other as soon as the VLAN defines ports to A and ports to B is belongs to different groups. Beyond that, over-lapping support can also be implemented to share other resources for both A and B at the same time.

To ease the installation, the Smart Switch supports proprietary port-based VLAN. The whole networks do not required any VLAN-aware devices like 3rd switches or applications.

VLT - VLAN-Trunk

Needed to transport multiple VLANs over one cable.

VxLAN - Virtual Extensible LAN

- RFC 7348
- Extends the limited amount of VLAN's by encapsulating Layer 2 packets into Layer-4-UDP packets.
- VLANs can be addresses the VLANID for about 4095 VLANs.
- With the VNI-ID in VxLAN over 16 Million addresses can be accessed.

VSAT - Very Small Aperture Terminal

Satellite dish (Ø 1m)

Firewall Types

Important FW Key Figures:

- App-ID FW throughput
- Threat prevention throughput
- IPSec VPN throughput
- Connections per second
- Max sessions (IPv4 or IPv6)

Trend: Hardware based firewalls ,

Circuit-Level Firewall

- Layer 4
- Functions on session-Layer.
- The Firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model.
- Less processing overhead as an Application Level Proxy.
- Monitor the TCP handshaking going on between the local and remote hosts to determine whether the session being initiated is legitimate -- whether the remote system is considered "trusted." They don't inspect the packets themselves, however.

Stateful Inspection Firewall

- Operates on network- and/or transport layer
- See also Stateful Packet Inspection (SPI).
- Only packets matching a known active connection will be allowed by the firewall.
- On the other hand, not only examine each packet, but also keep track of whether that packet is part of an established **TCP session**.

- This offers more security than either packet filtering or circuit monitoring alone but exacts a greater toll on network performance.

NGFW - Next Generation Firewall

Packet Filtering Firewall

WAF - Web Application Firewall

- Also called: **Anwendungsschicht-Gateway Firewall, Application-Level Gateway, Application-Proxy Firewall**

Vorteil: Verhindern, dass IP_Pakete einen Weg ins Netz schleusen.

Nachteil: Hohe laufende Kosten

Für jeden Dienst muss eine Proxy-Applikation konfiguriert werden.

- A **web application firewall** is a form of firewall which controls input, output, and/or access from, to, or by an application or service.
- It operates by monitoring and potentially blocking the input, output, or system service calls which do not meet the configured policy of the firewall.
- The application firewall is typically built to control all network traffic on any OSI layer up to the **application layer**.
- It can control applications or services specifically, unlike a stateful network firewall which is - without additional software - unable to control network traffic regarding a specific application.
- There are two primary categories of application firewalls, **network-based application firewalls** and **host-based application firewalls**.

Source: Wikipedia

- Eine Web Application Firewall (WAF) oder Web Shield ist ein Verfahren, das Webanwendungen vor Angriffen über das Hypertext Transfer Protocol (HTTP) schützen soll.
- Es stellt damit einen Spezialfall einer **Application-Level-Firewall (ALF)** oder eines **Application-Level-Gateways (ALG)** dar.
- Gegenüber klassischen Firewalls und "Intrusion Detection"-Systemen (IDS) untersucht eine WAF die Kommunikation auf der **Anwendungsebene**.
- Dazu ist normalerweise keine Änderung an der zu schützenden Web-Anwendung nötig.
- TIS Firewall Toolkit <ftp://ftp.tis.com/pub/firewalls/toolkit/dist>
- SOCKS <http://www.socks.nec.com/introduction.html>

Produkte: **F5, Netscaler** oder **AirLock**



Placemet Decision Tree

BorderWare Firewall Server 6.1

Sicherheit fürs Netzwerk

Preisübersicht & Bestellmöglichkeit

Wenn Sie Ihr Hausnetz ans Internet anschließen, öffnen Sie Hackern Tür und Tor zu Ihren Datenbeständen. Erst der Schutz per Firewall-Software (firewall, englisch = Brandmauer) sichert Ihr Netz gegen Eindringlinge und unbemerkten Datenklau.

Hohe Sicherheit für Ihr Netzwerk muß nicht teuer oder kompliziert sein. Speziell mit dem Augenmerk auf kleine und mittlere Netzwerke und Firmen, hat der Hersteller Borderware den Firewall Server auf den Markt gebracht.

Die Software ist einfach in Betrieb zu nehmen und leicht am Laufen zu halten. Sie verlangt weder aufwendige Spezialhardware noch teure Spezialisten. Borderware Firewall Server-Software sichert Ihr ans Internet angebundenes Netzwerk ab und wächst mit Ihrem Unternehmen und den Ansprüchen mit.

Artikelname	Preis
BorderWare Firewall Server 6.1 engl. 25-User	DM 5.908,-
BorderWare Firewall Server 6.1 engl. 50-User	DM 9.847,-
BorderWare Firewall Server 6.1 engl. Evaluation	DM 149,-

Checkpoint One

Fortinet

IPTables

- For Linux 2.4 kernel
- Is a Linux command line firewall that allows system administrators to manage incoming and outgoing traffic via a set of configurable table rules.
- Iptables uses a set of tables which have chains that contain set of built-in or user defined rules.

NOKIA

NOKIA IP440

- Breed of: CHECKPOINT ONE & CISCO ROUTER
- Configuration: Via normal Web-Browser
- Benötigt weder Monitor noch Tastatur.

Interfaces: bis zu 2,04 Mbit/s Ethernet, Fast Ethernet, ATM, FDDI, T1/E1, T3/E3,
 bis zu 45Mbit/s HSSI

WAN-Protokolle: PPP, CISCO HDLC, Frame Relay

Services: SNMP, MIB I, MIB II, TELNET, FTP

Routingprotocols: RIP1, RIP2, IGRP, OSPF, BGP-4, Multicast DVMRP
Router Redundancy Protocol (VRRP)

SonicWALL

TIS Firewall Toolkit

- WAF
- The Trusted Information Systems Firewall Toolkit (fwtk) is a very useful kit for creating bastion hosts.

Enthält Proxies für folgende Dienste:

Telnet
FTP
Rlogin
Sendmail
HTTP
X Window System

Watchguard

WEBRTC - Web Real-Time Communication

- License: **BSD license**
- With WebRTC, you can add real-time communication capabilities to your application that works on top of an open standard.
- It supports **video**, **voice**, and **generic data** to be sent between peers, allowing developers to build powerful voice- and video-communication solutions.
- **The technology is available on all modern browsers** as well as on native clients for all major platforms.
- The technologies behind WebRTC are implemented as an open web standard and available as regular **JavaScript APIs** in all major browsers.
- For native clients, like **Android** and **iOS** applications, a library is available that provides the same functionality.
- The WebRTC project is **open-source** and supported by Apple, Google, Microsoft and Mozilla, amongst others.
- WebRTC **encrypts** all data in transit.
- WebRTC is communication **between browsers** (Client to Client).
- WebRTC works over **UDP**.

WLAN

- 802.11b → 11 Mbit/s

- 802.11g → 54 Mbit/s
- 802.11n → 600 Mbit/s
- 802.11ac wird im 5 GHz Bereich bei neueren Geräten verwendet und erreicht bis zu 660 Mbit/s
- Das 2.4 GHz-Netz strahlt weiter, ist dafür aber langsamer wegen der eingeschränkten Bandbreite
- Das 5 GHz-Netz ist schneller, strahlt aber weniger weit. In der Regel ist das 5 GHz-Netz aber weniger belegt und bietet deshalb eine bessere Verbindung

Cisco APs can operate in two modes:

- Autonomous mode
- Lightweight mode

Autonomous Mode

- The AP operates independently and directly connects VLANs to WLANs on a one-to-one basis.

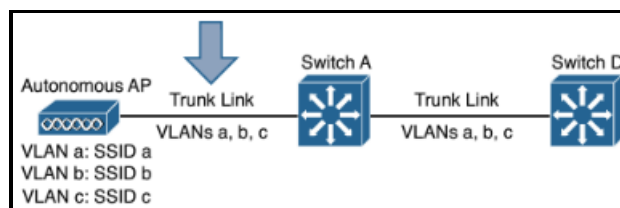


Figure 102: Autonomous Wireless AP

Lightweights Mode

- The AP must join and cooperate with a wireless LAN controller located elsewhere on the network. The AP connects each of its own WLANs with a VLAN connected to the controller. All of the VLAN-WLAN traffic is encapsulated and carried over a special tunnel between the AP and the controller.

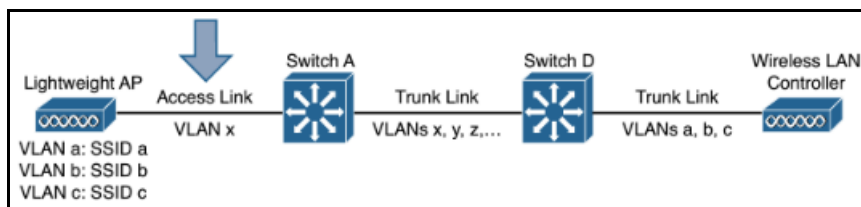


Figure 103: Lightweight Wireless AP

2.4 GHz-Frequenzband

Der Frequenzbereich im 2,4-GHz-Band wird in 13 Kanäle aufgeteilt. Obwohl der Kanalabstand 5 MHz beträgt, benötigt eine Funkverbindung eine Bandbreite von 20 MHz.

Die meisten Kanäle überlappen sich. Kanal 3 strahlt beispielsweise auch in Kanal 2 und 4. Daher werden oft die nicht-überlappenden Kanäle 1, 6 oder 11 verwendet. In gewissen Fällen kann es aber auch hilfreich sein, bewusst einen anderen Kanal zu verwenden.

Beispiel:

Wenn die Kanäle 1, 6 und 11 sehr stark belegt sind, sollte die Kanäle 3 oder 4 gewählt werden, da diese unbelegt sind.

5 GHz-Frequenzband

Der Frequenzbereich im 5-GHz-Band wird in 19 Kanäle aufgeteilt, zwischen Kanal 36 und 140. Obwohl im 5 GHz-Bereich normalerweise eine Kanalbreite von 40 MHz verwendet wird, überlappen sich die Kanäle nicht. Dies ermöglicht höhere Geschwindigkeit mit geringeren Interferenzen.

Generell haben die unteren Kanäle weniger Sendeleistung als die oberen. Die Kanäle zwischen 100

und 140 strahlen am weitesten (1000 mW, UNII-2 extended).

Bitte beachten Sie:

Beim Kanalwechsel in einen höheren Bereich kann es bis zu 10 Minuten dauern, bis die WLAN-Verbindung wieder hergestellt ist.

WPA

WPA2

WWW

- Is the @Internet's graphic interface, which is used to provide multimedia services.
- The WWW is made up of **Universal Resource Locators (URLs)**, which are different sites all over the world.

Syntax: <Protocol>:<Password>@<Host>:<Port>/<Path>

X.509 PKI

See also RFC 2459

CRL certificate revocation list

Filename extensions:

- .pem DER form, Privacy-enhanced Electronic Mail
- .cer .crt. .der DER form
- .p7b .p7c PKCS#7
- .p12 PKCS#12
- .pfx PKCS#12

Structure of a certificate:

- Certificate
- Version X.509, X509v3
- Serial Number
- Algorithm ID
- Issuer
- Validity
 - Not Before
 - Not After
- Subject
- Subject Public Key Info
 - Public Key Algorithm
 - Subject Public Key
- Issuer Unique Identifier (optional)
- Subject Unique Identifier (optional)
- Extensions (optional)
 - ...
- Certificate Signature Algorithm
- Certificate Signature

XFP Transceiver (XFP)

The **XFP** (10 Gigabit Small Form Factor Pluggable) is a standard for transceivers for high-speed computer network and telecommunication links that use optical fiber. It was defined by an industry group in 2002, along with its interface to other electrical components, which is called **XFI**.

XFP modules are hot-swappable and protocol-independent. They typically operate at near-infrared wavelengths (colors) of 850 nm, 1310 nm or 1550 nm.

RFCs

Links: <https://tools.ietf.org/html>
<https://tools.ietf.org/html/rfc9999>]

- 791 @Internet Protocol (**IP**)
- MTU
- 793 Transmission Control Protocol (**TCP**)
- 826 **Ethernet** Address Resolution Protocol
- 827 Exterior Gateway Protocol (**EGP**)
- 854 **Telnet** Protocol Specification
- 896 Nagle's Algorithm
- 904 Exterior Gateway Protocol formal specification
- 958 **NTP**
- 959 File Transfer Protocol (**FTP**)
- 1001 NetBIOS
- 1002 NetBIOS
- 1027 **Proxy ARP**
- 1065 Structure and identification of management information for TCP/IP-based internets
- 1122 MTU / **Nagle's** Algorithm
- 1157 Simple Network Management Protocol (**SNMP**)
- 1335 A Two-Tier Address Structure for the Internet:
- A Solution to the Problem of **Address Space Exhaustion**
- 1483 ???
- 1518 An Architecture for IP Address Allocation with **CIDR**
- 1519 Classless Inter-Domain Routing (**CIDR**)
an Address Assignment and Aggregation Strategy
- 1631 The IP Network Address Translator (**NAT**)
- 1661 The Point-to-Point Protocol (**PPP**)
- 1771 A Border Gateway Protocol 4 (**BGP-4**)
- 1860 Variable Length Subnet
- 1878 Variable Length Subnet
- 1918 Address allocation for **Private Internets** (private addresses)
- Running out of addresses
- 1930 Guidelines for creation, selection, and registration of an Autonomous System (**AS**)
- 1990 The **PPP** Multilink Protocol (**MP**)
- 2026 The **Internet Standards Process** -- Revision 3
- 2030 Simple Network Time Protocol (**SNTP**) Version 4 for IPv4, IPv6 and OSI.
- 2068 HTTP 1.1
- 2080 **RIPng** for IPv6
- 2273 **SNMPv3** Applications
- 2275 View-based Access Control Model (**VACM**) for the Simple Network Management Protocol (**SNMP**)
- 2338 Virtual Router Redundancy Protocol (**VRRP**)
- 2459 **X.509 PKI**
- 2460 @Internet Protocol, Version 6 (**IPv6**) Specification
- 2474 Definition of the Differentiated Services Field (**DS** Field) in the IPv4 and IPv6 Headers
- 2475 An Architecture for **Differentiated Services (DS)**
- 2597 Assured Forwarding **PHB** Group
- 2784 Generic Routing Encapsulation (**GRE**)
- 2865 Remote Authentication Dial In User Service (**RADIUS**)
- 3022 Traditional IP Network Address Translator (Traditional **NAT**)
- 3101 The OSPF Not-So-Stubby Area (**NSSA**) Option
- 3246 An Expedited Forwarding **PHB** (Per-Hop Behavior)
- 3330 ???
- 3947 NAT-Traversal
- 4193 **Unique Local IPv6 Unicast Addresses**
- 4301 IPsec
- 4380 Teredo
- 4632 Classless Inter-domain Routing (**CIDR**)
- 4890 Recommendations for Filtering **ICMPv6** Messages in Firewalls
- 5214 ISATAP
- 5340 ???
- 5415 CAPWAP

5424 The **Syslog** Protocol
5969 **IPv6 Rapid Deployment** on IPv4 Infrastructures
5798 VRRP
6127 **IPv4 Run-Out** and IPv4-IPv6 Co-Existence Scenarios
6333 **Dual-Stack Lite** Broadband Deployments Following **IPv4 Exhaustion**
6877 464XLAT
7123 **Security Implications** of IPv6 on IPv4 Networks
7230 Hypertext Transfer Protocol (**HTTP/1.1**): Message Syntax and Routing
7348 Virtual eXtensible Local Area Network (**VXLAN**)
7540 HTTP 2.0
7595 Guidelines and Registration Procedures for **URI Schemes**

DEFINITIONS

ACI - Application Centric Infrastructure

- Cisco Application Centric Infrastructure is Cisco's leading software-defined networking (SDN) solution, facilitating application agility and data center automation.
- Cisco ACI is traditionally deployed through a combination of other industry-leading solutions, including the Cisco Nexus 9000 Series data center switches, the Cisco Application Policy Infrastructure Controller (APIC), and other hardware and software solutions.

Terms:

- Contract
- EPG Customer
- EPG Provider

Videos:

[Introduction to Cisco Application Centric Infrastructure - What It Is](#)
[Cisco HyperFlex & Veeam Availability solutions](#)

CCP - Cisco Container Platform

???

COPS - Common Open Policy Service

- Cops is used in a client/server model where the server is a policy server or policy decision point (PDP) and the client is a policy enforcement point (PEP).

SDA - Software Defined Access

- See also SDN

Secure routing protocols

See: [Cisco Network Security Baseline](#)

- Secure routing protocols in ad hoc networks are the protocols designed to counteract **routing attacks that disrupt route discovery**.

DWDM - Dense Wavelength Division Multiplexing

- **Dense Wavelength Division Multiplexing (DWDM)** is an optical multiplexing technology used to increase bandwidth over existing fiber networks. DWDM works by combining and transmitting multiple signals simultaneously at different wavelengths on the same fiber.
- In fiber-optic communications, wavelength-division multiplexing (WDM) is a technology which multiplexes a number of optical carrier signals onto a single optical fiber by using different wavelengths (i.e., colors) of laser light.
- This technique enables bidirectional communications over one strand of fiber, as well as multiplication of capacity.
- The technology creates multiple virtual fibers, thus multiplying the capacity of the physical medium.

Split DNS - Split Domain Name System

- Is an implementation in which **separate DNS servers** are provided for **internal and external networks** as a means of security and privacy management.
- In this implementation, whenever a user sends a request for an administrative network resource and makes the request from the same network, the internal DNS handles name resolution.

- However, if the same user requests the same resource from an external network, the external DNS handles the resolution that provides a certain abstraction from the internal network where the resource is located.
- Split DNS is also known as ***split-horizon DNS*** or ***split-view DNS***

Abbreviations

ACL	Access Control List
ACRC	Advanced Cisco Router Configuration
APIC-EM	Application Policy Infrastructure Controller Enterprise Module
ASA	Adaptive Security Appliance
ASIC	Application Specific Integrated Circuit (Layer 2)
AVR	Active Virtual Router
BDD	Binary Decision Diagram (see ACL)
BSCI	Building Scalable Cisco Internetworks
BRI	Basic Rate ISDN - Basisanschluss 2 B-Kanäle mit 64kbps und einme D-Kanal 16kbps
CAM	Content Addressable Memory
CATV	Community Antenna Television
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CLI	Command Line Interface
CLM	Cisco License Manger
CoS	Class of Service
CST	Common Spanning Tree
CVD	Cisco Validated Design
DAI	Dynamic ARP inspection
DCE	Data Communication Equipment
DLCI	Ein DLCI pro Endknoten eines PVC im Frame Relay (Logical Channel bei X.25)
DLSw	Data Link Switching
DMZ	Demilitarized Zone
DNA	Digital Network Architecture
DoS	Denial of Service (DDoS Distributed Denial of Service Attack)
DRAM	Dynamic Random-Access Memory
DTE	Data Terminal Equipment
DTP	Dynamic Trunk Protocol
DUAL	Diffusing Update Algorithm
ELSR	Edge Label Switch Router
ESA	Cisco Enterprise Service Automation
EUI	Extended Unique Identifier (IPv6)
FIB	Forwarding Information Base
FSM	Finite State Machine (See: BGP)
GLBP	Gateway Load Balancing Protocol
HSM	Harware Security Module
IARP	Inverse ARP
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISL	Inter/Switch Link
ISP	Internet Service Provider
ISR	Integrated Services Router
IVR	Inter-VLAN Routing
LLQ	Low Latency Queuing
NAT	Network Address Translation
NDE	NetFlow Data Export
NIM	Network Interface Module
NMS	Network Management Station
NVRAM	Non Volatil Random Access Memory (Startup-config)
OSPF	Open Shortest Path First
PAT	Port Address Translation (NAT Overload)
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
PPPoA	Point-to-Point Protocol over ATM
PRI	Primary Rate ISDN - Primärmultiplexanschluss T1 oder E1
RIB	Routing Information Base (simple the IP routing Table)
RQL	Root Link Query Protocol
RTM	Routing Table Manager
ROAS	Router on a stick
SAF	Cisco Service Advertisement Framework
SCP	Secure Copy

SLA	Summary Link Advertisements
STUN	Serial Tunnel for Front End Processors (IBM)
SVI	Switched Virtual Interface (see also IVR)
TACACS	Terminal Access Controller Access-Control System
UDI	Unique Device Identifier
VLSM	Variable Length Subnet Mask
VoIP	Voice over Internet Protocol
VTP	VLAN Trunk Protocol (transparent mode)
VTS	Virtual Topology System

Table of Figures

Figure 1: Cisco Certification Path	13
Figure 2: Multinode Core	20
Figure 3: Multi-Tier Architecture.....	21
Figure 4: Three-Tier Architecture.....	22
Figure 5: Typical Components of an enterprise Network.....	23
Figure 6: Fully Redundant Hierarchical Network Design	23
Figure 7: A Redundant Core Layer	24
Figure 8: Multi-Node Core in a very large Campus Network	24
Figure 9: Collapsed Core network design	25
Figure 10: Switch Block.....	26
Figure 11: Traditional three-tier network design.....	26
Figure 12: Leaf-Spine architecture design	26
Figure 13: Network Summarization.....	27
Figure 14: OSI Layers	29
Figure 15: OSI versus TCP/IP	29
Figure 16: DOD and OSI Model.....	29
Figure 17: Bandwidth Delay Product (BDP)	38
Figure 18: DSLAM.....	39
Figure 19: Data Encapsulation	39
Figure 20: Encapsulate TCP/UDP	43
Figure 21: Numbers and Sizes of Class A, B and C Networks	45
Figure 22: Multicast Traffic	46
Figure 23: Broadcast Network Type	47
Figure 24: Privileged Exec mode commands.....	54
Figure 25: uRPF - Strict Mode.....	61
Figure 26: TACACS+ and RADIUS Server	62
Figure 27: SNMP Components.....	63
Figure 28: SNMP Security Models.....	63
Figure 29: #show flash	64
Figure 30: IP Helper Address	66
Figure 31: show cdp neighbors.....	68
Figure 32: show cdp neighbors detail	68
Figure 33: Ethernet Frame.....	76
Figure 34: EtherChannel	76
Figure 35: Port Security Modes	79
Figure 36: Interface Statuses.....	82
Figure 37: show vlan	89
Figure 38: show vlan brief.....	89
Figure 39: show interface trunk.....	90
Figure 40: Extended ACL	96
Figure 41: PAT Topology.....	99
Figure 42: Basic NAT Topology	100
Figure 43: IPv6 Header	103
Figure 44: IPv6 Address example.....	103
Figure 45: IPv6 Prefix assignment in the @Internet	104
Figure 46: IPv6 Global Unicast Address	106
Figure 47: IPv6 Address Assignment.....	106
Figure 48: Link Local FE80::/10	106
Figure 49: IPv6 Stateless Autoconfiguration	109
Figure 50: ipv6 address autoconfig default	109
Figure 51: ICMPv6	111
Figure 52: Neighbor Solicitation (NS/NA).....	111
Figure 53: Router Solicitation RS/RA.....	112
Figure 54: Duplicate Address Detection (DAD).....	112
Figure 55: 6to4 Tunnel	113
Figure 56: STP Overview	115
Figure 57: BPDU Frame Format.....	117
Figure 58: Guidelines for applying STP Protection Features.....	119
Figure 59: VRRP	127
Figure 60: NetFlow Inspection.....	133
Figure 61: Relationship for Path Control using IP SLA.....	136
Figure 62: Jitter	137
Figure 63: NBMA Network Type	149
Figure 64: LSA Types.....	152
Figure 65: Hub and Spoke Network.....	153
Figure 66: OSPF Stubby Area Types.....	153

Figure 67: show ip interface brief.....	155
Figure 68> show ip ospf neighbor.....	158
Figure 69: OSPF single area.....	159
Figure 70:OSPF multi area.....	159
Figure 71: BGP Update Message.....	162
Figure 72: Dual-Homed Design Options.....	165
Figure 73: Single-Multihomed Designs.....	165
Figure 74: Dual-Multihomed Options.....	166
Figure 75: Find BGP PA Settings.....	167
Figure 76: BGP Decision Process (N WLLA OMNI).....	168
Figure 77: Influencing Best Path.....	168
Figure 78: WAN Terms.....	172
Figure 79: CPE and CSU.....	172
Figure 80: WAN Connection Types.....	174
Figure 81: CHAP authentication sequence.....	180
Figure 82: Sample EVN Topology.....	186
Figure 83: Programmability Stack.....	191
Figure 84: Where APIC EM fits in the SDN stack.....	192
Figure 85: Logical Architecture.....	192
Figure 86: QoS Strategy.....	193
Figure 87: Cisco Unified Computing System.....	195
Figure 88: UCS XML API Features.....	195
Figure 89: IPv6 Address Assignment for Global Unicast Addresses.....	196
Figure 90: Details of the RS/RA Process.....	196
Figure 91: Comparing Stateless and Stateful DHCPv6 Services.....	196
Figure 92: GRE Tunnel.....	200
Figure 93: GRE over IPSec Tunnel.....	200
Figure 94: Hub-and-Spoke mGRE tunnel topology.....	201
Figure 95: Spoke-to-Spoke mGRE tunnel topology.....	201
Figure 96: Point-to-Point Network Type.....	203
Figure 97: Broadcast Domain.....	223
Figure 98: DNS Round Robin.....	227
Figure 99: Typical MTU-Sizes.....	233
Figure 100: SFP.....	240
Figure 101: TCP/IP Stack.....	245
Figure 102: Autonomous Wireless AP.....	252
Figure 103: Lightweight Wireless AP.....	252

Index

<i>802.1Q</i>	80	NetBT	234
AAA	62	NPAS	236
ADSL	182	NPS	236
APNIC	221	OCSP	224
ARP	203	OSPF	147
ASN	222	PaaS	241
ATS	238	PAgP	76
AVG	125	PAP	179
BaaS	241	PAT	98
BGP	71, 72, 161, 222	PKI	224
BID	117	PPPoE	181, 182
CA	224	RA	236
CEF	70	RIP	71, 72, 73, 239, 245
CHAP	179	RIPv1	72
CIR	176, 200	RIPv2	73, 74, 75
CPE	172	ROAS	80
CRL	253	Root-Switch	116
CSU	172	RSPAN	243
DaaS	241	RTD	220
DAI	122	RTT	220
Dijkstra	147	SaaS	240, 241
DNSBL	226	SCEP	239
DNSSEC	227	SCP	212
DoS	226	SDH	242
DSU	172	SDN	191
EDGE	228	SDSL	242
EGP	71	SFP	239
FC	228	SLAAC	102, 107, 212
FCoE	228	SMB	242
FHRP	125	SMLT	244
FTPS	228	SONET	242
GLBP	125	SPAN	242
GRE	199, 200	SPI	248
HSDPA	229	STP	241
HSRP	125	SVI	86, 87
IaaS	241	Teredo	245
IAS	236	TLS	246
ICAP	230	TPM	246
ICMP	202, 203	UMTS	247
IFS	53	VDSL	247
IGP	71	VHDSL	247
ISATAP	230	VLAN	247
ITMaaS	241	VLSM	52, 247, 259
Jabber	231	VoIP	199
Jitter	137	VRF	185, 186
LACP	77, 232	VRRP	125
LTPA	231, 232	VTP	91
MEF	232	VVID	87
MLT	244	VXLAN	255
MPLS	233	WAF	249
MTU	232	WAS	229
NAT	98	WPA	253
NBT	234	WRED	47
ND	212	XFP	253
NDES	236		