IP Network

WAN Architecture

ACKNOWLEDGEMENT

This lecture material was developed with primary references to:

Cisco Smart Business Architecture

While the focus of this lecture is on the architecture of WAN and internetworking, some of the concepts provided here are exclusively owned by Cisco SBA, its purpose is to shift the idea from the older and convoluted to the newer and simplified technology and business approaches.

Disclaimer: They may not be responsible to the accuracy of this material.

Overview

- Organization grows and adapts to business requirement and activity
- Requires transparent access to the applications and files
  - Flexible network design even for organizations with presence in different geographical locations, especially country-specific
- Considerations to performance, reliable service level and broad availability of carrier provided transport technologies, specifically
  - MPLS
  - Layer 2

Goal

- Provide consistent user experience
- Users through the facility (the network) can increase productivity
- WAN must provide sufficient performance and reliability
  - Make common workforce's access to the resources regardless of location
  - Supports convergence of voice, video and data transport into a centrally managed infrastructure
- Flexible (check hierarchical layer) design of the network
  - Reduce time needed to deploy new technologies
  - Support emerging business applications and communications
  - Easily scale bandwidth, add new additional sites or resilient links
  - Establish not so costly backup or option to primary transport technology
- Controls, compare and monitors cost

WAN tranports

- MPLS
- Layer 2
- Internet VPN
- Cellular technology or 3G/4G VPN

Multi-Protocol Label Switching

- Enables organizations and service providers to build next-generation intelligent networks
- Delivers a wide variety of advance, value added services like QoS and SLA (service level agreements)
- Integrates seamlessly over any existing infrastructure such as IP, frame relay, ATM and Ethernet
- MPLS L3 uses peer-to-peer VPN model
  - Leverages BGP to distribute VPN related information
  - Allows customers to outsource routing information to service providers
  - Can results to significant cost savings and reduced operational complexity for organizations

Multi-Protocol Label Switching cont'n

- Enable Multicast VPN to transport IP multicast
- Serves as
  - Primary MPLS
  - Backup MPLS
- Supports both
  - Ethernet over MPLS (EoMPLS)
  - Virtual Private LAN Service (VPLS)

Layer 2

- Uses Ethernet
  - Traditionally been a LAN technology primarily due to the distance limitations of the available media
  - Requirement for dedicated copper and fiber links
- Widely available from service providers
- Extends various L2 traffic
  - PPP
  - FR
  - ATM
  - Ethernet

Layer 2 cont'n

- Most common implemetations
  - Ethernet over WAN
    - Point to point service
    - Point to multipoint service
- Providers other network technologies in various topologies with Ethernet
  - Carrier Ethernet or Metro Ethernet
    - Typically limited to a relatively small geographic area
    - Organization (or customer) implements all L3 routing
  - Allows flexibility in the WAN design and interconnection of the remote sites

Layer 2 cont’n

- Transparent to the traffic type
  - I.e. multicast traffic is supported with no additional configuration required, especially, by service provider

Layer 2, point to point service

- Allows for the interconnection of 2 LANs (or sites)

Layer 2, point to multipoint transparent LAN service

- Allows for the interconnection of more than 2 LANs (or sites)

Layer 2, trunked service or Q-in-Q tunneling

- Uses trunk mode
- Interconnects LAN using 802.1Q
  - VLAN tagging
    - Provides transport of multiple VLANs on a single access trunk

Layer 2 WAN aggregation design models

- Uses single WAN edge router, most popularly called as CE
- Design models are either
  - Simple demarcation, or
  - Trunk demarcation
- Design models differ on
  - The number of broadcast domains or VLANs that are used to communicate with a subset of remote site-routers
- Uses LAN connection into either
  - Collapsed core/distribution layer, or
  - Dedicated WAN distribution layer
- No functional differences between these 2 models from that WAN-aggregation perspective
- IP route summarization are performed at the distribution layer
- Various devices supporting WAN edge services are performed at the distribution layer

L2 WAN aggregation design models

	L2 Simple Demarcation	L2 Trunk Demarcation
Remote sites	Up to 25	Up to 100
WAN links	Single	Single
Edge routers	Single	Single
Routing protocol	EIGRP	EIGRP
Transport 1 type	MetroE/VPLS	MetroE/VPLS
Transport 1 demarcation	Simple	Simple

Layer 2 trunk demarcation

- Logically separates remote-sites peering
- Distributes router peers across multiple VLANs
  - Maximum of 25 remote-site router peers per VLAN
- Typical in dedicated WAN distribution layer

Virtual Private Network

- Internet Protocol
- Dynamic Multipoint

Internet (as WAN)

- Best effort, nature
- Reasonable choice for a primary transport
  - When no feasible transport option is available
- Provides additional resiliency for primary WAN transports like MPLS or L2
- Typically included in discussions relevant to Internet edge
  - Specially for primary site
- Access at remote sites often routed through primary site
  - Security reasons

Dynamic Multipoint VPN

- Considered a solution for building scalable site-to-site VPNs
  - Widely used for encrypted S2S connectivity over private or public IP networks
- Supports variety of application including
  - On demand full mesh connectivity with
    - Hub-and-spoke configuration, and
    - Zero touch hub deployment model for adding remote sites
  - Spoke routers that have dynamically assigned IP addresses

DMVPN, mGRE (sometimes mGRE tunnels)

- Multipoint Generic Routing Encapsulation
  - Interconnects the hub of all the spoke routers
- Referred to as DMVPN clouds
- Supports (re technology combination)
  - Unicast
  - Multicast
  - Broadcast
  - Run routing protocols within the tunnels

VPN WAN

- Transport options include traditional
  - Internet access used either
    - Primary transport
    - Secondary transport when the primary is MPLS. L2
- Single or dual carrier Internet access links connect to
  - VPN hub router
  - VPN hub router pair
    - Similar method of connection and configuration is used for both

VPN WAN design models

- DMVPN only – uses only Internet VPN as transport
- Dual DMVPN – uses Internet VPN as primary and secondary with dual internet service providers (ISP)
- DMVPN backup – uses Internet VPN as backup to primary existing MPLS or L2 WAN tranports
  - Differences
    - DMVPN backup shared – the VPN hub is implemented on an existing MPLS CE router
    - DMVPN backup dedicated – the VPN hub is implemented on a dedicated VPN hub router
- Said design models uses LAN connections into either a collapsed core/distribution or dedicated distribution layers
  - WAN aggregation perspective, no functional difference between these methods
  - IP route summarization at the distribution layer

VPN transport-only design models

	DMVPN Only	Dual DMVPN
Remote sites	Up to 100	Up to 500
WAN links	Single	Dual
DMVPN hubs	Single	Dual
Transport 1	Internet VPN	Internet VPN
Transport 2	---	Internet VPN

VPN transport backup design models

	DMVPN backup shared	DMVPN backup dedicated
Remote sites	Up to 50	Up to 100/500
WAN links	Dual	Multiple
DMVPN hubs	Single (shared with MPLS CE)	Single / Dual
Transport 1 existing	MPLS VPN A	MPLS VPN A
Transport 2 existing	---	MPLS VPN B
Transport 3 existing	---	MetroE/VPLS
Backup transport	Internet VPN	Internet VPN

Cellular

- Enables use of Internet WAN
  - Without requiring wired infrastructure and circuits
- Provides a flexible, high-speed, high-bandwidth option
- Competing 3G technologies
  - CDMA
  - GSM
- 4G technologies include
  - LTE
  - WIMAX

Quality of Service

- Enables multitude of user services to co-exist within the same network
  - Real time voice
  - High quality video
  - Delay sensitive data i.e. stock market pricing
- Provides
  - Advance classification
  - Prioritization
  - Queuing
  - Congestion mechanism
- Helps ensure optimal use of network resources
- Allows for the differentiation of applications
  - Ensures that each has the share of the network resources
- Protects users experience
- Ensures consistent operations of business critical applications

QoS

- Provides services that are
  - Predictable
  - Measurable
  - Guaranteed (sometimes)
- Manages
  - Bandwidth
  - Delay
  - Jitter
  - Loss parameters

QoS exclusive of network

- Manages and protects
  - Network protocols, functionality and manageability, under normal and congested traffic conditions

WAN aggregation design models

- MPLS: static, dynamic, dual
- L2: simple and trunked demarcations
- DMVPN:
  - DMVPN only
  - Dual
  - Backup shared
  - Backup dedicated

MPLS WAN design

- WAN aggregation includes 1 or 2 edge routers
  - Can be statically or dynamically routed with either single or dual MPLS carriers
- Customer edge (CE) routers
  - Referred to in the context of the connection to a carrier or service provider
- WAN edge routers connect to a LAN distribution layer
- MPLS VPN used as primary or secondary transport
  - Each transport connects to a dedicated CE router
  - Similar method for connection and configuration for both applies

MPLS WAN design continuation

- Differences between various designs are
  - Usage of routing protocols
  - Overall scale of the architecture
  - Router platforms to choose from with differing levels of performance and resiliency capabilities
- Design models uses LAN connection into either a
  - Collapsed core/distribution layer
  - Dedicated Wan distribution layer
    - No functional difference between this two methods from WAN aggregation perspective

MPLS WAN design continuation

- Remember: IP route summarization are performed at the distribution layer
- Various devices supporting WAN edge services, see the following, should connect to the distribution layer
  - Application optimization i.e. traffic, load balance
  - Encryption i.e. IP security or Internet VPN
- MPLS carrier terminates to a dedicated WAN router with a primary goal:
  - ELIMINATING A SINGLE POINT OF FAILURE

MPLS WAN aggregation design models

	STATIC	DYNAMIC	DUAL
Remote sites	Up to 50	Up to 100	Up to 500
WAN links	Single	Single	Dual
Edge routers	Single	Single	Dual
Routing protocol	None (static)	BGP (dynamic)	BGP (dynamic)
Transport 1	MPLS VPN A	MPLS VPN A	MPLS VPN A
Transport 2	---	---	MPLS VPN B

WAN remote sites design

- Most remote sites are designed with a single router WAN edge
- Certain remote site types require a dual router WAN edge, include
  - Regional office
  - Remote campus locations with large user populations
  - Site with business critical needs that justify additional redundancy to remove single points of failure
- Routing specification is tied closely to the bandwidth required for a location and for the potential requirement for the use of service module slots

WAN remote-site transport options

WAN remote site routers	WAN transports	Primary transport	Secondary transport	WAN aggregation design model (primary)	WAN aggregation design model (secondary)
Single	Single	MPLS VPN	---	MPLS static, MPLS dynamic, Dual MPLS	---
Single	Single	MetroE/VPLS	---	L2 simple, L2 trunked	---
Single	Single	Internet	---	DMVPN only, Dual DMVPN	---
Single	Single	Internet 3G/4G	---	DMVPN only, Dual DMVPN	---
Single	Dual	MPLS VPN A	MPLS VPN B	Dual MPLS	Dual MPLS
Single	Dual	MPLS VPN	Internet	MPLS static, MPLS dynamic, Dual MPLS	DMVPN backup shared, DMVPN backup dedicated
Single	Dual	MPLS VPN	Internet 3G/4G	MPLS static, MPLS dynamic, Dual MPLS	DMVPN backup shared, DMVPN backup dedicated
Single	Dual	MetroE/VPLS	Internet	L2 simple, L2 trunked	DMVPN backup dedicated
Single	Dual	Internet	Internet	Dual DMVPN	Dual DMVPN
Dual	Dual	MPLS VPN A	MPLS VPN B	Dual MPLS	Dual MPLS
Dual	Dual	MPLS VPN	Internet	MPLS dynamic, Dual MPLS	DMVPN backup dedicated
Dual	Dual	MPLS VPN	Internet 3G/4G	MPLS dynamic, Dual MPLS	DMPVN backup dedicated
Dual	Dual	MetroE/VPLS	Internet	L2 simple, L2 trunked	DMVPN backup dedicated
Dual	Dual	Internet	Internet	Dual DMVPN	Dual DMVPN

MPLS WAN connected remote site compatibility

- MPLS WAN non-redundant variant
  - The only one that is compatible with the single carrier design models (MPLS static or dynamic)
- MPLS WAN redundant variant
  - Dual MPLS design, may also connect a non-redundant remote site to either carrier

VPN WAN connected remote site compatibility

- Internet WAN non-redundant variant
  - DMVPN only and dual DMVPN
- Internet WAN redundant variant
  - Dual DMVPN design
- MPLS + Internet WAN single router (redundant links) variant
  - Either DMVPN backup dedicated or DMVPN backup shared
- MPLS + Internet WAN dual router (redundant links and routers) and both L2 WAN + Internet WAN variants
  - DMVPN backup dedicated

3/4G VPN WAN connected remote site compatibility

- Internet WAN non-redundant variant
  - DMVPN only and dual DMVPN
- MPLS + Internet WAN single router (redundant links) variant
  - Either DMVPN backup dedicated or DMVPN backup shared
- MPLS + Internet WAN dual router (redundant links and routers) and both L2 WAN + Internet WAN variants
  - DMVPN backup dedicated

Remote site WAN/LAN interconnection

- Primary role of the WAN (*specific details about LAN components was discuss in IP network, LAN/WAN fundamentals or with Cisco SBA the LAN deployment guide*)
  - Interconnect primary (HQ/main office) site to remote-site LANs

WAN remote site LAN options

WAN remote site routers	WAN transports	LAN topology
Single	Single	Access only, Distribution/Access
Single	Dual	Access only, Distribution/Access
Dual	Dual	Access only, Distribution/Access

WAN remote site LAN topology

- Uses VLAN
- Relevant to any location that has single access switch
- Can be easily scaled, as model as this, to additional access by adding distribution layer

WAN remote sites VLAN assignments

VLAN	Usage	L2 access	L3 distribution / access
VLAN v	Data 1	Yes	---
VLAN w	Voice 1	Yes	---
VLAN x	Transit	Yes (dual router only)	Yes (dual router only)
VLAN y	Router Link (1)	---	Yes
VLAN z	Router Link (2)	---	Yes (dual router only)

WAN/LAN remote site interconnection, L2 access

- Do not require additional LAN distribution layer routing devices
  - Considered flat or in LAN perspective unrouted L2 site
- For routing, it is the job of the WAN router that provide all L3 services
- Access switches, through multiple VLAN can support services
  - Data
  - Voice
- Access switches can be configured (*see LAN deployment guide for the complete configuration*) identically regardless of the number of sites
- Remember 802.1Q VLAN trunking

WAN/LAN remote site interconnection, L2 access--dual-router edge

- Similar LAN design can be extended
- The change in the design introduces additional complexity
- Requirements
  - Run routing protocol—Enhanced Interior Gateway Routing Protocol (EIGRP)—between routers
  - With 2 routers per subnet now must implement—First Hop Redundancy Protocol (FHRP)—however, with Cisco selected Hot Standby Rotuer Protocol as its application to FHRP
    - Designed to allow for transparent failover of the first-hop IP router
    - Provides high-network availability with first hop routing redundancy for IP hosts configured with a default gateway IP address

WAN/LAN remote site interconnection, L2 access--dual-router edge--FHRP

- Used in a group of routers for selecting an active and standby router
  - When there are multiple routers in LAN, the active router is the router of choice for routing packets
  - The standby router takes over when or when the active router fails or when preset conditions are met
- Designed to allow for transparent failover of the first-hop IP router
- Provides high-network availability with first hop routing redundancy for IP hosts configured with a default gateway IP address

WAN/LAN remote site interconnection, L2 access--dual-router edge—FHRP cont'n

- Enhanced Object Tracking (EOT) provides a consistent methodology for various router and switching features to conditionally modify their operation based on information objects available within other processes
- Object that can be tracked includes
  - Interface line protocol
  - IP route reachability
  - IP service level agreement (SLA) reachability

WAN/LAN remote site interconnection, L2 access--dual-router edge—IP SLA

- Provides a capability for a router to generate synthetic network traffic that can be sent a remote responder—it can be a generic IP endpoint that can respond to
  - ICMP request or
  - Cisco router running an IP SLA responder process—can respond to more complex traffic such as jitter probes
- Allows router to determine end-to-end reachability to a destination and also the roundtrip delay
- Permits calculation of loss and jitter along the path in more complex probe types
- This design uses IP SLA in tandem with EOT

WAN/LAN remote site interconnection, L2 access--dual-router edge—IP SLA and EOT tandem

- Improves convergence time after a primary WAN failure
- Through use of this tandem
  - HSRP has the capability to monitor the reachability of a next-hop IP neighbor
  - Allows a router to give its HSRP active role if its upstream neighbor becomes unresponsive
- Provides additional network resiliency

WAN/LAN remote site interconnection, L2 access--dual-router edge—IP SLA probe

- HSRP is configured to be active on the router with the highest priority WAN transport
- EOT is implemented in conjunction with HSRP
  - The standby HSRP router (alternate) becomes active in the case of WAN failure
- Sent from the remote-site primary WAN router to the upstream neighbor (MPLS CE, L2 WAN CE, DMVPN hub) to ensure reachability of the next-hop rotuer
- More effective than simply monitoring the status of the WAN interface

Dual router designs, referred to as the hairpinning

- Warrants additional transit network component that is required for proper routing (in certain scenarios)
- Cases
  - A traffic flow from a remote-site host might be sent to a destination reachable via the alternate WAN transport (a dual MPLS remote site communicating with an MPLS-B-only remote site). The primary WAN transport router then forwards the traffic back out the same data interface on which it was received from the LAN to send it to the alternate WAN transport router, which then forwards the traffic to the proper destination

Dual router designs, avoid hairpinning

- Introduce additional link between the routers and designate the link as a transit network (*remember VLAN assignments or check out WAN design overview page 21*)
- No hosts connected to the transit network
  - Only used for router-to-router subinterfaces assigned to the transit network
- No additional router interfaces are required this design modification
  - 802.1Q VLAN trunk configuration can easily accommodate an additional subinterface

WAN/LAN remote site interconnection, distribution and access layers

- Large remote sites may require a LAN environment similar to that of a small campus LAN
  - Topology such as this works well with either a single- or dual-router WAN edge
- Routers should connect via EtherChannel links to the distribution switch (to implement this design)
- EtherChannel links are configured as 802.1Q VLAN trunks to support both

WAN/LAN remote site interconnection, distribution and access layers—EC links

- Are configured as 802.1Q VLAN trunks to support both
  - Routed point to point link to
    - Allow EIGRP routing with the distribution switch
  - Dual-router design to
    - Provide a transit network for direct communication between the WAN routers

WAN/LAN remote site interconnection, LAN distribution switch

- Handles all access layer routing
  - With VLANs trunked to access switches
- No HSRP is required when the design includes a distribution layer

WAN remote site—distribution and access layers (dual router)