Convergence in Metro Area Networks

Randall Atkinson
rja@extremenetworks.com
Chief Scientist

extreme networks

Agenda

- What are converged networks ?
- Why is convergence happening ?
- How does this change Metro Area Networks (MANs) ?
- Key technologies enabling MAN convergence
  - Need to have Quality of Service, Resilience, & Scalability
- Deployment considerations

Terminology

- A traditional network only provides best-effort service. It is designed to carry packet data and is not designed specifically for real-time or prioritised data.
- A converged network supports multiple priorities and service qualities. It is designed to carry not only ordinary packet data, but also multimedia traffic, for example IP Telephony, and other real-time traffic.

Why Converge Networks ?

- Reduce end-user costs
  - Easy to convince users to switch to lower-cost IP-based provider from higher-cost TDM-based provider
- Reduce service-provider costs
  - Eliminates need to build and maintain an expensive TDM network in parallel with the Ethernet/IP network
  - Reduced operations & maintenance costs
- Improve service provider business
  - Additional product/service offerings are possible
  - Delivers more revenue from a single network infrastructure

Ethernet drives Convergence

- Ethernet is the dominant link-layer technology today
  - Virtually all VoIP handsets use Ethernet
  - Virtually all enterprises use Ethernet for their LANs
- Lower cost than traditional TDM technologies
- Recent advances in Ethernet enable convergence
  - 10 Gigabit Ethernet now widely available, 40 GigE coming
    - Lower cost than SONET/SDH, compatible with WDM systems
  - Ring Topologies for resilience (RFC-3619)
  - Ethernet Quality-of-Service (IEEE 802.1p)
  - VLANs (IEEE 802.1q), VMANs, & MPLS for scalability
- Easy to configure, operate, and manage
  - Results in lower recurring operational expenses

IP Telephony Drives Convergence

- Converged networks permit service providers to broaden their markets
  - Can offer telephone service in addition to packet service
  - Can offer video-conferencing services also
  - Can offer their packet network service for higher rates
  - In future, could also sell IP Television to compete with cable television
- Price bundling can lure customers to obtain more services from a single converged provider

Video Drives Convergence

- IP Video Conferencing increasingly deployed by enterprise users
  - Lower cost than ISDN
  - No Advance Circuit Provisioning is Needed
  - Can use multimedia appliance or leverage existing PCs
- Telecom firms interested in new services
  - Microsoft investing heavily in IP/TV initiative
  - Verizon (USA) deploying trial for IP/TV
- *Triple-Play for IP Telephony, IP Video, and IP data*
  - Delivered over a single converged network
  - Billed together on a single monthly statement
  - Captures more revenue from existing customers

Customers Drive Convergence

- Enterprise customers are converging their networks
  - IP Storage is increasingly popular
    - Lower-cost, more resilient, more flexible than older approaches
  - Voice-over-IP is increasingly popular within enterprises
    - Initial deployment normally for internal phone calls
    - Can lead to significant cost reductions just for intra-company phone calls
  - Internal video-conferencing is moving from ISDN to IP
- Enterprise customers need improved service quality from their service providers
  - Enables the intra-company convergence initially
  - Converged network operators are better able to compete

Business Issues

Business Models: Comparison

- Traditional Packet Data Network
  - Best-effort service only, no QoS mechanisms
  - Pricing based only on the access network speed
  - Tiered-services based only on access network speeds
  - Easily commoditised, hurting profit margins
- Converged Voice/Data Network
  - Service Quality becomes a differentiator
  - Pricing based on access network speed and QoS
  - Broader range of service offerings becomes possible
  - Service Quality protects against commoditisation
  - Better profit margins are possible

Business Models: Enterprise

- Basic Enterprise service
  - Enterprise customer with multiple locations
  - Provides only basic IP service to each location
  - Customer deploys their own VPN service
  - Best-Effort delivery of IP packets
  - No support for carrying customer VLAN tags across the IP network
  - Highly commoditised
  - Competing on price

- Enterprise VPN service
  - Enterprise customer with multiple locations
  - Enterprise customer delivers internal VoIP traffic on a separate link/port/VLAN-ID from their packet data traffic
  - Provides layer-2 VPN service between sites
  - Voice/video traffic gets preferred service quality
  - Not commoditised
  - Competing on services and quality, not price

extreme networks

Business Models: IP Telephony

- Packet telephone services using VoIP
  - Uses IP Telephony end-to-end, with VoIP soft-switch and PSTN interconnection provided by service provider
  - QoS markings are added at the provider-edge switch, based on address of the IP telephone handset(s)
  - Enables broader deployment of telephony services
  - Reduces cost of deploying telephony to new customers
  - Reduces cost of capacity within the service provider network
- Traditional telephone services using VoIP
  - Use traditional telephony between PBX/CO and the customer
  - Use IP Telephony between the PBXs and COs internally
  - Reduces cost of capacity within the service provider network
  - Easier to deploy and lower risk, but also less benefit

Business Models: IP/Video

- Cable TV companies already offer Triple-Play
  - Telephony, Video, and Data on a single monthly bill
  - Telephony, Video, and Data over common HFC deployment
  - Customers like ability to get all services from one provider
- Traditional Telecom firms
  - Offer Traditional Telephony
  - Offer Data services via DSL
  - Now can offer television, moves, and other video over IP
- Deploying IP/Video Services enables traditional Telecom firms to compete more effectively

Application Issues

Potential Voice/Video Issues

- Voice/video quality can be very sensitive to:
  - Packet Loss
  - Delay (also called Latency)
  - Jitter (also called Variation in Delay)
- Traditional data traffic is not very sensitivity to moderate amounts of packet loss, delay, or jitter
- So a Converged Network needs several enhancements to support all kinds of applications.

Voice/Video Encoder Issues

- Many voice encoder (vocoder) algorithms have been standardised
  - Examples: ITU-T G.711, ITU-T G.729, CELP for voice
  - Examples: MPEG3, MPEG4 for video
  - Both ITU-T and IETF have specified vocoder algorithms
- Different algorithms have different properties
  - Many older algorithms were designed for circuit networks and do not work as well in packet networks
  - Example: ITU-T G.729 requires about half the bandwidth of ITU-T G.711 for nearly the same voice quality
  - Different algorithms are more tolerant or less tolerant of jitter, delay or loss.
- Need to use an appropriate algorithm !

Enterprise VPN Issues

- Many enterprises are deploying IP Telephony (VoIP) within the corporate LAN
- Some enterprise applications are more important
  - Example: Database is more important than IM or Email
- Enterprises want higher service quality for their most important VPN traffic
- Enterprises use VLANs across multiple sites
- Service provider implications:
  - Quality, not price, becomes the key differentiator
  - Converged metro networks with Layer-2 VPN service can be an important new offering for enterprise customers

Other Service Quality Issues

- Not all data applications are equally important
  - Example: Database access is usually much more important than instant messaging to enterprise users
  - Example: IP Storage works best with low delay and low packet loss rate
  - Example: web browsing is often not very important
- Need to ensure that mission-critical applications receive the best quality of network service.
- Need to be able to protect the service provider network from QoS-centric Denial-of-Service (DoS) attacks.

How does the MAN change ?

- Traditional MANs have been built upon:
  - Best-effort IP service
  - Best-effort Ethernet service
  - VLANs to separate users
  - Fault recovery times from 1 second to several minutes
- Converged MANs also require:
  - IP Quality-of-Service
  - Ethernet Quality-of-Service
  - Virtual MANs or Hierarchical VPLS for Layer-2 VPNs
  - Fault recovery as quickly as ~50ms
  - Enhanced switch/router capabilities

Enabling Technologies for Converged Networks

Metropolitan Area Ethernet

- Key enabling technology for metro convergence
    - Lower cost, compatible with Enterprise LANs, easy to manage
- Key Advances in Ethernet Technology
    - Scalability from 10 Mbps to 10 Gbps, and in future 40 Gbps
    - Ethernet Quality-of-Service (IEEE 802.1p)
        - Protect real-time voice/video traffic
    - VLANs (IEEE 802.1q) & VMANs (802.1q in 802.1q)
    - Ethernet Automatic Protection Switching (RFC-3619)
        - Protection against fibre cuts (approx 50ms recovery time)
    - Jumbo Frames
        - Larger than IEEE standard allows
        - Enables tunnelling and encapsulation without fragmentation

extreme networks

Scalability: Virtual MAN & MPLS

- Issues:
  - IEEE 802.1q standard only supports 4k VLAN IDs
  - Service providers need to support more than 4k customers with a Metro Area Network
- Layer-3 VPNs can not help with this problem
  - Layer-3 VPNs can’t carry the layer-2 VLAN IDs end-to-end
- Two technology approaches are commonly used:
  - Virtual MANs (VMANs)
    - Double VLAN encapsulation -- IEEE 802.1q in IEEE 802.1q
  - MPLS Layer-2 VPNs
    - Hierarchical Virtual Private LAN Service (H-VPLS)

Quality of Service: Design Options

- Over-provisioning Capacity
  - If no congestion, then no problems from delay, jitter, or loss
  - Can be very cost-effective with “dark fibre” deployments
- Ethernet Precedence
  - Originally specified in IEEE 802.1p
  - Provides 3 bits to mark each Ethernet frame
- IP Type-of-Service, IP Precedence, IP DiffServ
  - 3 different names for essentially the same mechanism
- IETF Integrated Services with RSVP
  - Failed attempt to define QoS for IP networks during 1990s
  - RSVP protocol did not and does not scale sufficiently !

Quality of Service: Mechanisms

- QoS has 2 primary components
  - 1) QoS markings on packets
  - 2) Special packet processing in switches and routers
- Standards for QoS Markings
  - IETF Differentiated Services (DiffServ) from RFC-2475
  - IETF IP Type-of-Service (ToS), from RFC-791
  - IEEE Ethernet Precedence, from IEEE 802.1p
- Packet Processing Algorithm Examples
  - IETF DiffServ AF or EF queuing/forwarding
  - Weighted RED (WRED)
  - Weighted Fair Queing (WFQ)
  - Strict Precedence

IP Differentiated Services

- Most recent definition for the IP ToS byte
  - Backwards-compatible with IP Precedence
  - Defined by RFC-2474 and RFC-2475
- Defines 2 packet processing schemes
  - “Assured Forwarding” (AF), defined by RFC-2597
  - “Expedited Forwarding” (EF), defined by RFC-2598
- QoS Implementation details do matter
  - Works best when QoS is implemented in ASIC hardware, rather than in software on the main CPU

IP Queuing: AF versus EF

- Myth:
  - AF and EF are always very different from each other
- Reality:
  - When QoS and forwarding are implemented in ASIC hardware, there is little difference between AF and EF.
  - When QoS or forwarding are implemented in software on a CPU, there can be big differences between AF and EF

IP Queuing: only AF xor EF

- Myth:
  - There are only 2 possible configurations on a given queue
  - One can choose either AF xor EF packet handling
- Reality:
  - Better quality implementations have many configuration options, so AF and EF terminology is too restrictive.
  - Examples of other possible configuration parameters:
    - Minimum/Maximum bandwidth allocations to a flow or queue
    - Minimum/Maximum bandwidth allocations to a port or VLAN
    - Tuning parameters for WFQ or WRED
    - Clipping vs Rate-Limiting vs Rate-Shaping
    - Precedence

IP Queuing: VoIP Myth

- Myth:
  - VoIP requires EF packet processing; AF just won't work
- Reality:
  - VoIP requires thoughtful queuing
  - Either AF or EF can work well or work badly depending on the details of the implementation and configuration
  - Hardware-based QoS works best for any queuing algorithm
  - Other deployment details (Resiliency, Scalability, Capacity) remain very important

Quality of Service Model

- Each deployment needs to define a QoS Model
  - Defines how various kinds of traffic are categorised
  - Defines how each category is handled by switches/routers
- Highest Priority group is always “network control”
  - Essential traffic to keep the network up and running
  - Includes Bridging, IP Routing, SNMP, etc.
- Multimedia group higher than other applications
  - Includes SIP, MGCP, RTP, etc.
  - Signalling is higher priority than media packets
- Fine-grained QoS models work better
  - Best to have 8 or more hardware queues per port
  - Best to have flexible configuration options

extreme networks

Deployment Considerations

Resiliency: Ethernet Rings

- Why do we want rings ?
  - Often matches the actual deployed fibre topology
  - Rings can recover very quickly from fibre cuts
  - Positive experience with FDDI and SONET rings
- Normally, Ethernet cannot have a ring topology
  - Spanning Tree algorithm requires tree/branch topology
  - Loops in the topology prevent proper bridge convergence
- Ethernet Automatic Protection Switching (RFC-3619)
  - Enables Ethernet Ring network deployments
  - Works with standard Spanning Tree algorithms/protocols
  - Works with equipment from multiple vendors on the ring
  - Fast recovery from fibre cut: ~50ms

IP Telephony

- IP Telephony services benefit from special treatment
- Separate telephony from ordinary traffic using VLANs
- Ensure appropriate service quality
  - Mark telephony signalling & voice packets at the edge
  - Apply QoS queuing in the core, with ASIC-based QoS
  - Reserve bandwidth for telephony traffic in edge and core
  - Monitor port utilisation and link utilisation
- Ensure high availability for IP Telephony servers
  - SIP or H.323 servers need to be available 24x7x365
  - Use multi-homed servers and redundant servers
- Use non-blocking switches and routers

Operational Security

- Harden the network infrastructure
  - Eliminate clear-text passwords using Secure Shell (SSHv2)
  - Centralise/automate password management
    - Diameter, RADIUS, TACACS+, LDAP, and/or Kerberos
  - Use SNMPv3 with cryptography
    - SNMPv1 and SNMPv2c lack cryptographic security
- Enable thoughtful logging and auditing
  - Use automated tools to analyse logs and audit records
- Monitor traffic patterns and utilisation
  - Essential to detect and prevent attacks, abuse, and fraud
  - Alarm when specified thresholds are reached
- Emerging Stds: IETF OpSec WG

Configuration Management

- Scalability requires automation
  - "People are expensive, automation is cheap" - M. Medin
- Accuracy requires automation
  - Computers good at repeating the same task precisely
  - People make mistakes
- Typical Approach to Automation
  - Create and maintain network configuration database
  - Create and use automated tools to ensure actual equipment configuration matches the configuration database and report any differences between actual and expected configs
- Emerging Stds: IETF Network Configuration WG

Summary

What drives convergence ?

- Key Enabling technologies
  - Metro Area Ethernet
  - IP Telephony
- Customer demand
  - both from enterprise users & from residential users
- Business Concerns
  - Lower cost of deploying network, compared with TDM
  - Lower cost of operating network, compared with TDM
  - Additional revenue
  - Better profit margins
  - Better competitive position

Recommended Approach

- Select an appropriate business model
- Apply Converged Network design principles
  - High Service Quality
  - Resilience
  - Scalability
  - Availability
- Select equipment carefully
- Deploy thoughtfully after lab testing and trial(s)
- Minimise Total Cost of Ownership (TCO)
- Maximise revenue opportunities

Thank You