



Convergence and its Challenges

Extending Beyond IP Telephony

Manfred Arndt
HP Distinguished Technologist - Convergence Solution
May 23, 2007



Convergence Trends

IP video is poised to transform businesses



IP Telephony & Unified Messaging

- Reduced operating expense
- Enhanced productivity



IPTV and VoD

- New revenue opportunities
- Distance learning

Scalable/Adaptive Infrastructure



VoWLAN & Mobility

- Flexibility and agility
- Always connected



Telepresence & Visual Collaboration

- More effective communication
- Improved business outcome
- Dramatically cut travel expense



IP Video Security

- Enhanced physical security
- Advanced video analytics
- Crime and terrorism deterrent

Heightened global security concerns Market Opportunity

Physical and logical security market estimated at \$22 billion by 2010¹

City of London has over 2,000,000 video cameras deployed



Sao Palo violent crime rate went from #1 to #17 in one year

- Plan in place to expand from 60 to 1,000s of IP video cameras

Rio de Janeiro was able to reduce crime by 54% to 78% depending on area by installing 220 wireless IP video cameras

149 US cities have plans underway (39 cities have some video)

1 - Forrester Research and Giga Information Group.

Traffic types and IP addressing

Choosing which type to use and when is critical to insure that the network operates efficiency, especially for video

Unicast

- Single sender, single receiver
- Most commonly used transmission scheme on the Internet today

Broadcast

- Same packet sent to all connected receivers on a given LAN
- Excessive use can result in disastrous network bandwidth problems

Multicast

- Same packet sent to many receivers and can cross routers
- An extremely efficient distribution mechanism; since only one copy of every packet traverses any given link

Video Solution Types

Video on Demand

- Pay-per-view, distance learning, interactive TV
- Typically delivered as unicast data and buffered by client for smooth playback

Telepresence and Visual Collaboration

- Virtual meetings and real-time collaboration for greater productivity, improved business outcomes and reduced travel expensive
- Video conferencing is primarily unicast based, with one stream in each direction

IPTV

- Digital television over an IP network for lower cost and enhanced capabilities
- Deployed as multicast from a “few” content servers at the network core or distribution layer

Video Security

- Enhanced security with advanced capabilities over an open standards IP network
- Frequently deployed using multicast streams from “many” cameras at the edge of the network, expected to run 24/7

Video Network Requirements

	Voice ¹	Streaming Video (e.g. IPTV, VoD)	Video Conferencing	Video Security
Bandwidth requirements (per stream)	30-100 Kbps	100-500 Kbps (low) 500-3 Mbps (fair) 3-6 Mbps (DVD)	2-6 Mbps (standard) 12-45 Mbps (hi-def)	300 - 2 Mbps (or more with megapixel cameras)
Packet loss tolerance ²	Some loss tolerated < 1%	Some loss tolerated < 1% (Retransmitted with TCP)	Some loss tolerated < 1%	Some loss tolerated < 1%
Jitter tolerance	< 50 ms	Very High	< 50 ms	High
Delay tolerance	< 150 ms	Very High	< 250 ms	High
Key network requirements	QoS Reliability	Bandwidth Multicast (IPTV)	Bandwidth QoS	Network Planning High Performance Multicast Support Reliability

1. Voice guidelines as per ITU G.114 standard (for toll quality voice)

2. With packet loss concealment techniques, higher voice and video loss rates can be tolerated

How do Multicast Groups work?

- Who is part of what group?
- How do you join and leave?
- How does the network forward packets?

Each specific multicast stream uses a unique class D destination IP address that represents a unique multicast group

IGMP (Internet Group Management Protocol)

- Used by hosts to establish multicast group memberships with routers and switches

PIM (Protocol Independent Multicast)

- Used by routers to establish which multicast groups should be forwarded between VLANs and neighboring routers

Key IGMP terms

Multicast Group:

- A set of hosts, routers, and/or switches that send or receive a specific multicast data stream
- Switches and routers maintain multicast group tables to selectively forward packets only to ports as needed

IGMP Host:

- End stations that runs multicast applications utilizing IGMP
- Hosts send “join” and “leave” requests to specific multicast groups

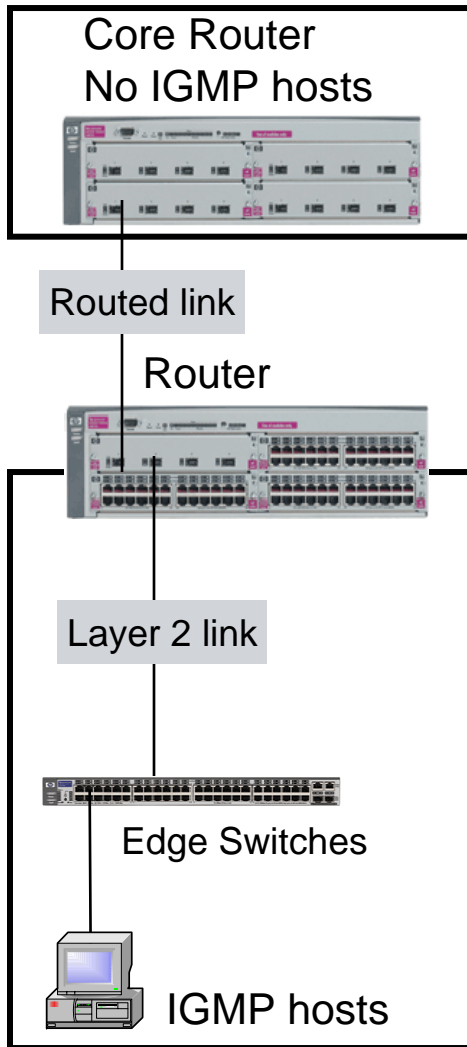
IGMP Snooping:

- Switches that listen to IGMP to discover active multicast receivers

IGMP Querier:

- IGMP routers (or switches) that sends requests and collects responses, to discover the location of multicast receivers

Multicast protocol requirements



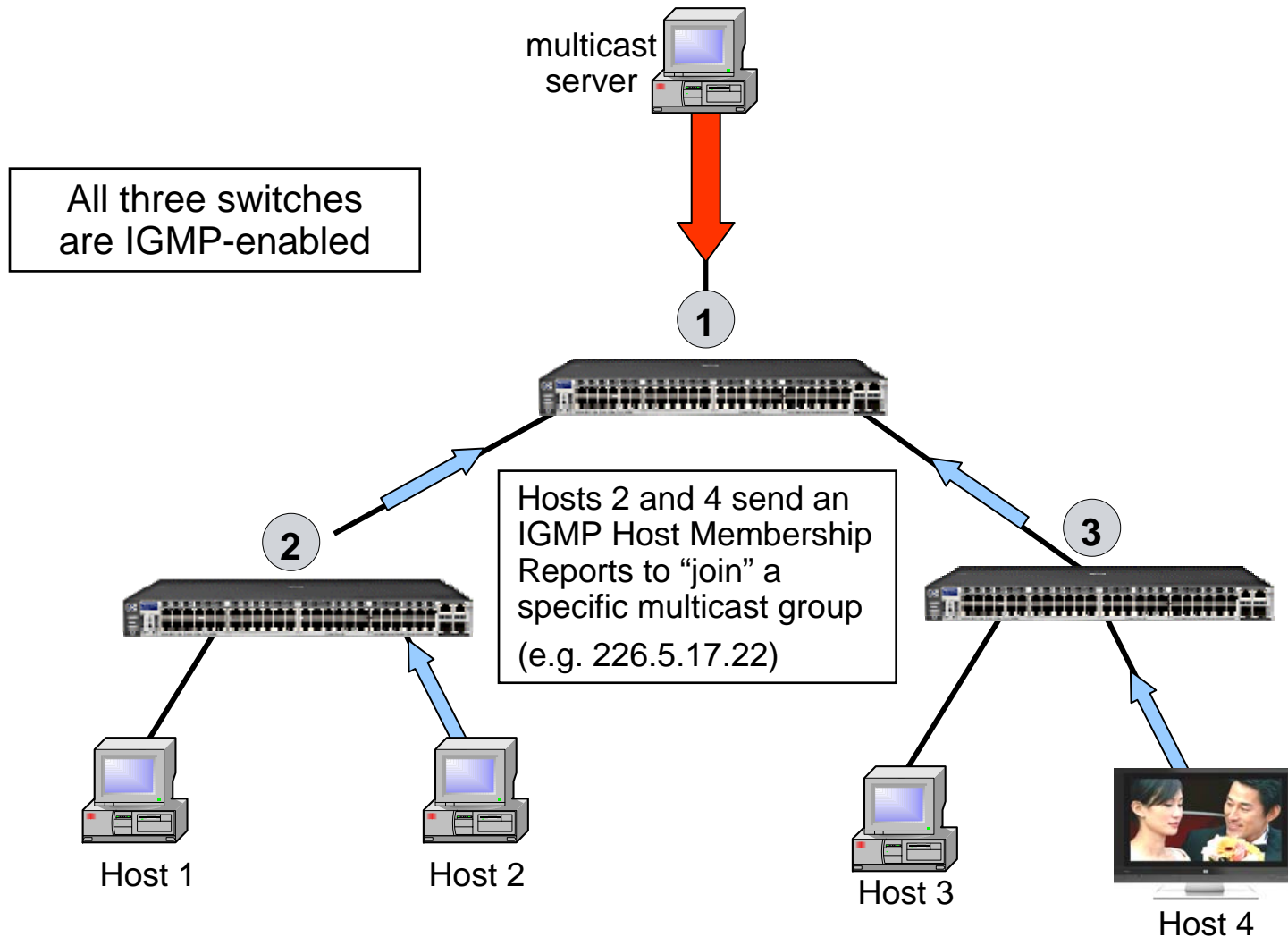
Core routers:

- Unicast routing protocol and/or static routes to build unicast route table (e.g. OSPF, RIP, static)
 - PIM uses unicast route tables to find best path
- PIM must be enabled for each VLAN with multicast
- IGMP must be enabled for each VLAN that will carry multicast traffic

Edge switch (Layer 2 only):

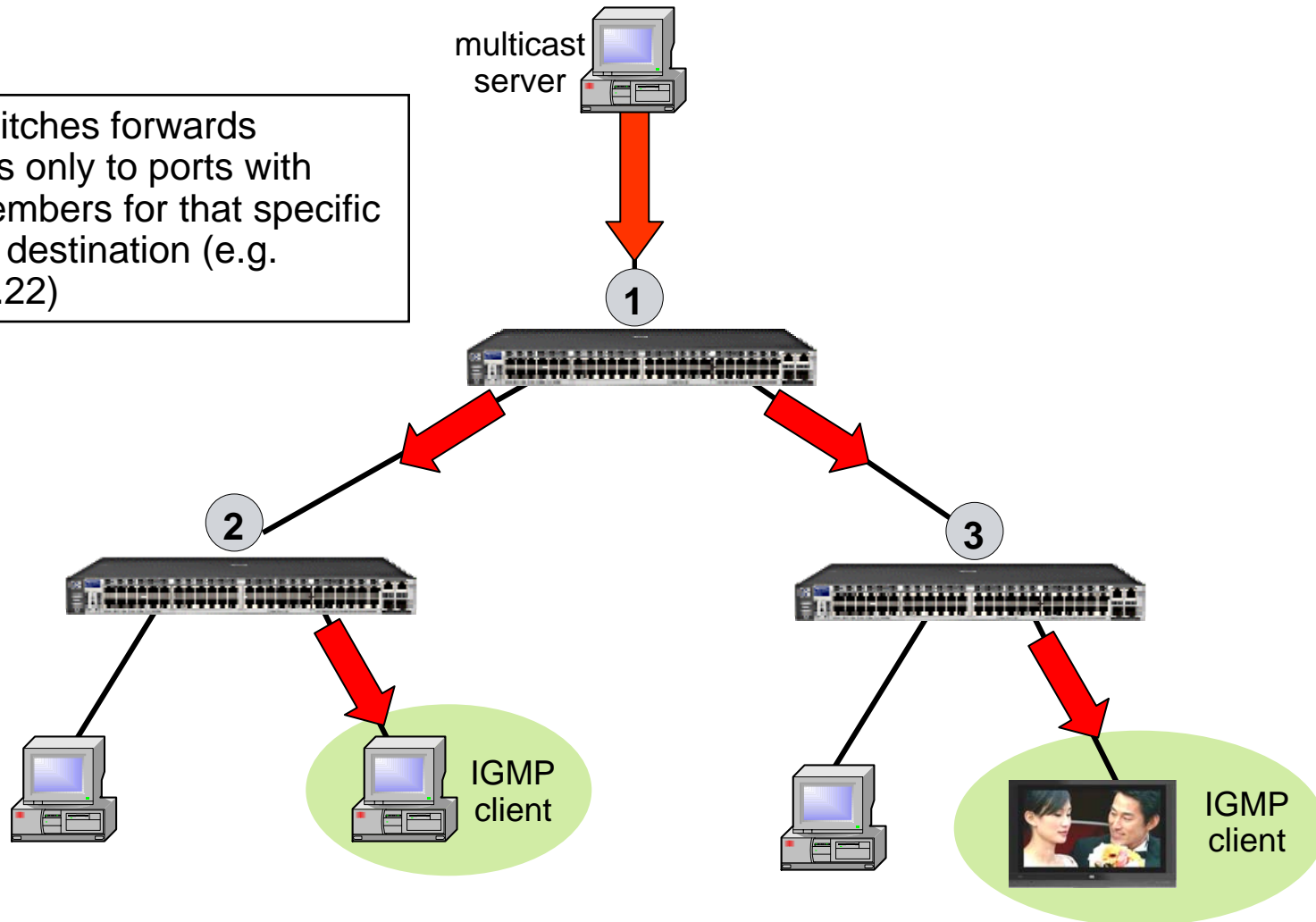
- IGMP must be enabled for each VLAN that will carry multicast traffic

IGMP host "join" example

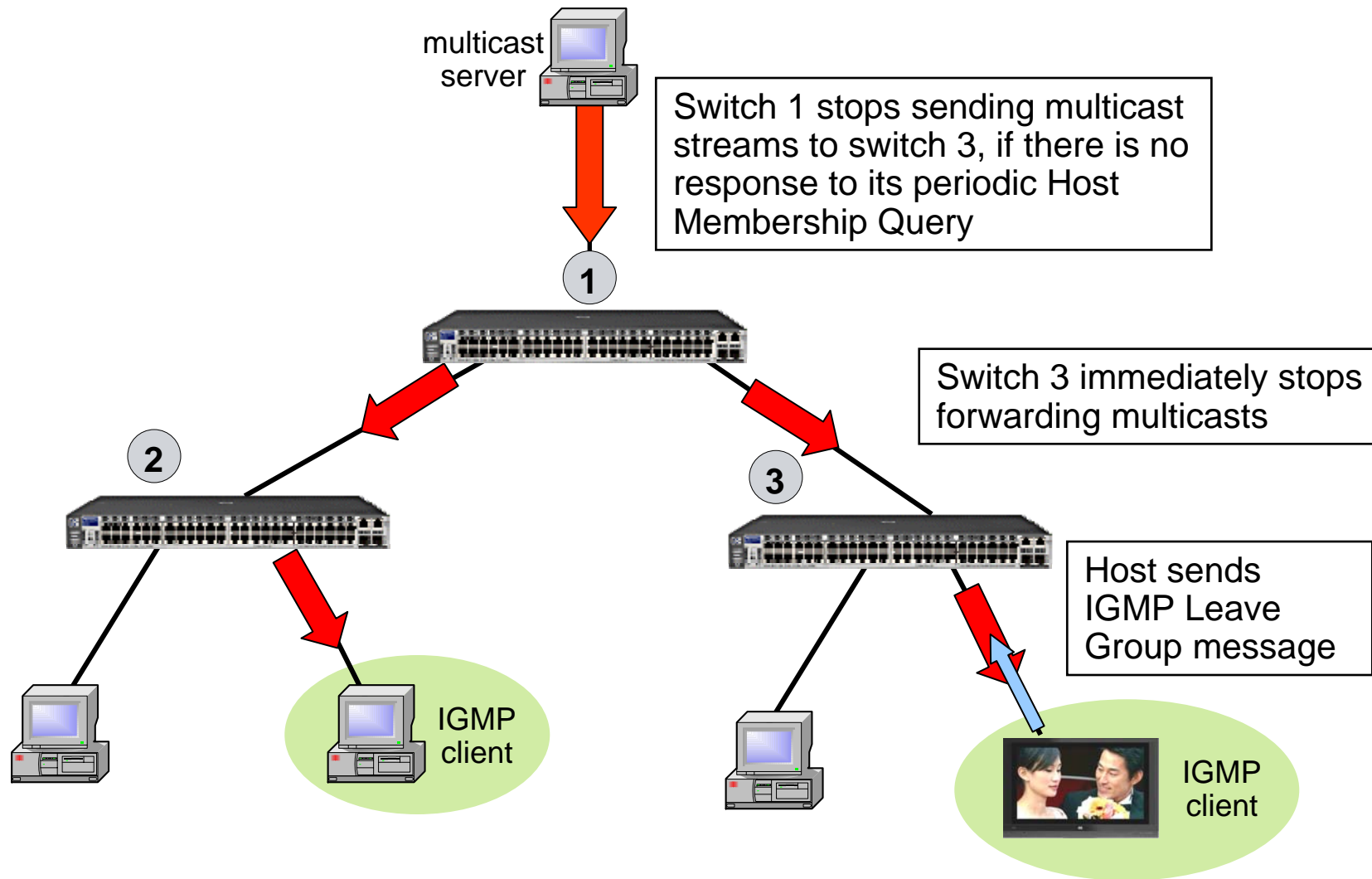


IGMP multicast forwarding

IGMP switches forwards multicasts only to ports with group members for that specific multicast destination (e.g. 226.5.17.22)



IGMP Fast-Leave



PIM comes in two flavors

PIM is a routing protocol to establish which multicast groups should be forwarded between VLANs and neighboring routers

Dense Mode (PIM-DM)

- Membership assumed until traffic is pruned
- Best for smaller deployments, with few multicast streams
- Periodically floods multicasts everywhere until traffic is pruned
- Results in periodic high traffic when there are many streams

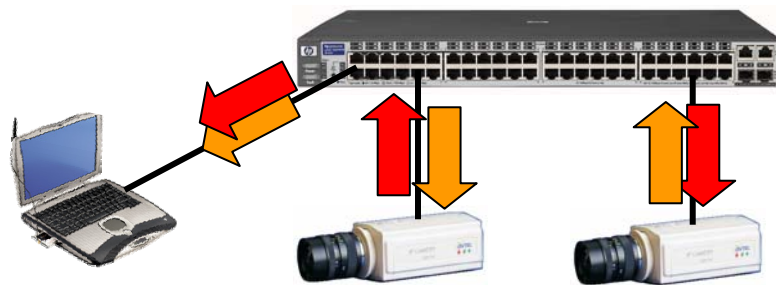
Sparse Mode (PIM-SM)

- Membership must be explicitly requested by receiver
- Optimized for many data streams and frequent changes
- Better scalability for large deployments

Not all switches are equal

Switches without proper IGMP flood multicasts on all ports

- IP cameras do not send IGMP “joins” and the standard does not define how to handle this, so some vendor switches flood this traffic
- Certain switches support **data-driven IGMP** to detect “unknown” multicast groups and block them appropriately
- Many switches have limited multicast group tables sizes and will flood all additional multicast streams
- Can result in ***serious performance*** issues, even for modest video solutions, due to the high bandwidth per video stream



Without data-driven IGMP, video from all cameras will flood every active port. This is because video cameras act as servers and rarely do IGMP “joins”.

Steps for successful deployment



Regardless of project size, the basic design steps are:

1. Assess requirements
2. Evaluate existing network and capabilities
3. Develop and propose a solution
4. Implement and document the solution

Assessing video requirements

Considerations Checklist:

- ✓ Number of end devices (cameras, servers, viewing stations, etc)
- ✓ Power-over-Ethernet (PoE) budget
- ✓ Cabling distance limits
- ✓ Number and location of wiring closets
- ✓ Ethernet port types and quantities
- ✓ Video quality and frame rate desired
- ✓ Location of high traffic servers, archivers, and viewing stations
- ✓ Calculate worst-case throughput needs at various network points
- ✓ Use VLANs to segment multicast traffic and improve scalability
- ✓ Multicast and routing requirements
- ✓ Applications requiring QoS prioritization
- ✓ Security and network access control requirements
- ✓ Availability requirements

Anticipate growth in the network

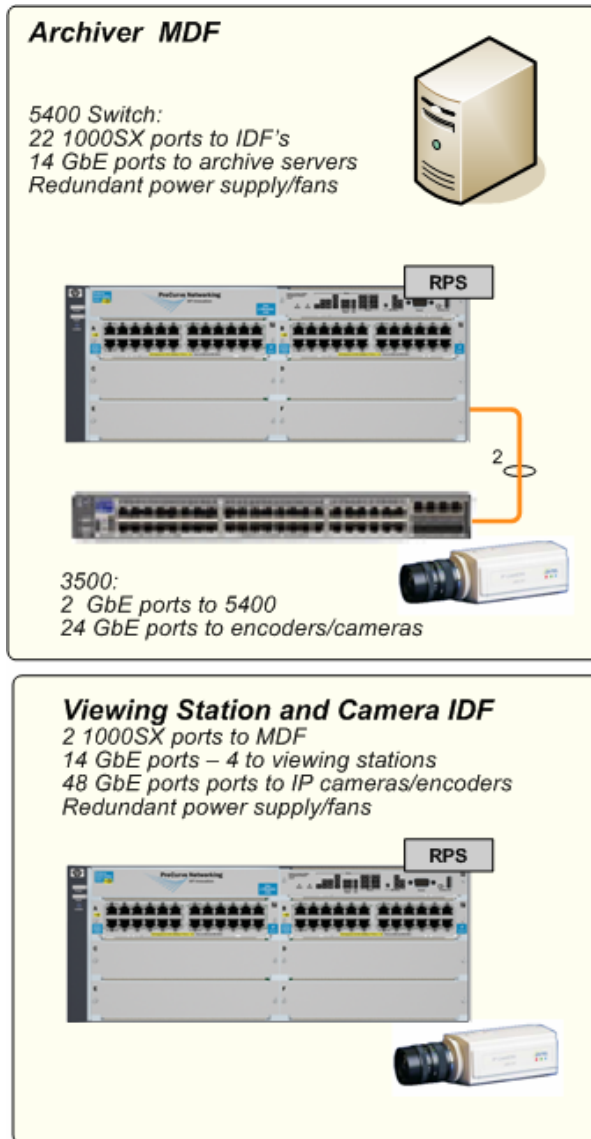
Implement and document solution



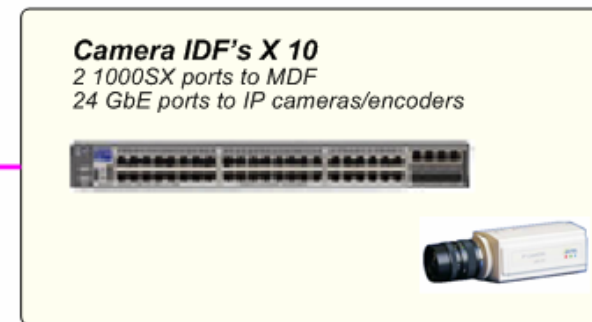
Configuration steps:

- Change passwords to prevent unauthorized access
- Define VLANs
- Assign IP subnets to VLANs
- Enable IGMP on all multicast VLANs
- Configure unicast routing (OSPF, RIP, or static)
- Multicast routing (PIM-DM, PIM-SM)
- Enable high availability as needed (RSTP/MSTP, VRRP, meshing,...)
- Define QoS prioritization
- Enable remote management
- Configure ACL's at Layer 3 boundaries
- Define network access security policies (802.1X or MAC Auth)
- Document as you work!

Large video security example



- Trunked 10 GbE uplinks
- 12 GbE archive servers
- 4 GbE viewing stations
- 2,600 IP cameras powered w/ PoE



- ProCurve 5400 core and aggregation
- 54 ProCurve 3500 edge switches
- Copper and fiber uplinks
- Redundant power supplies (RPS)

Key Takeaways

Many new applications likely to be added to your networks in the near future:

- IP phones and desktop video conferencing
- High-definition video collaboration
- IP video security cameras (100 to 1000s)



Plan ahead with an adaptive network infrastructure capable of:

- Flexible Layer 2 and Layer 3 QoS
- Power over Ethernet (PoE)
- Mechanisms to control and prioritize high aggregate multicast traffic at full line rate
- Rate limiting with guaranteed minimum bandwidth
- Multicast routing with data-driven IGMP
- Open standards-based interoperability





ProCurve Networking

HP Innovation