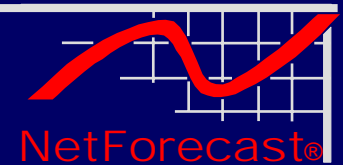


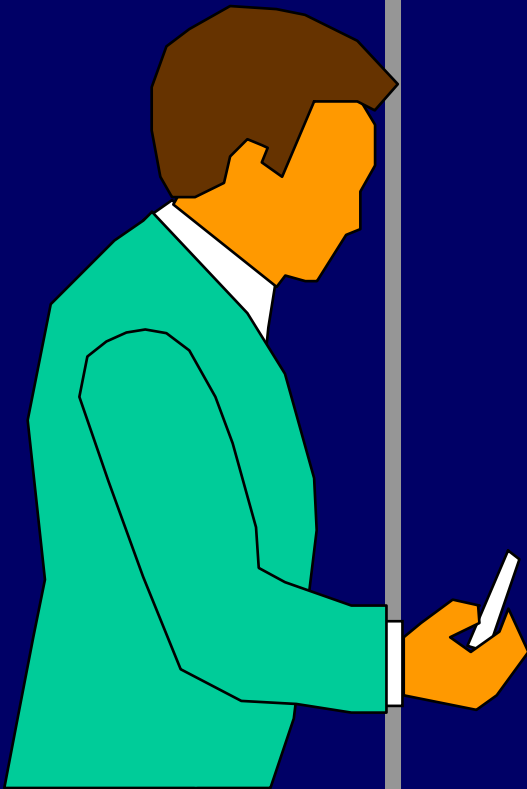
Implementing Multimedia Conferencing

InterOp Las Vegas
4-May-2006

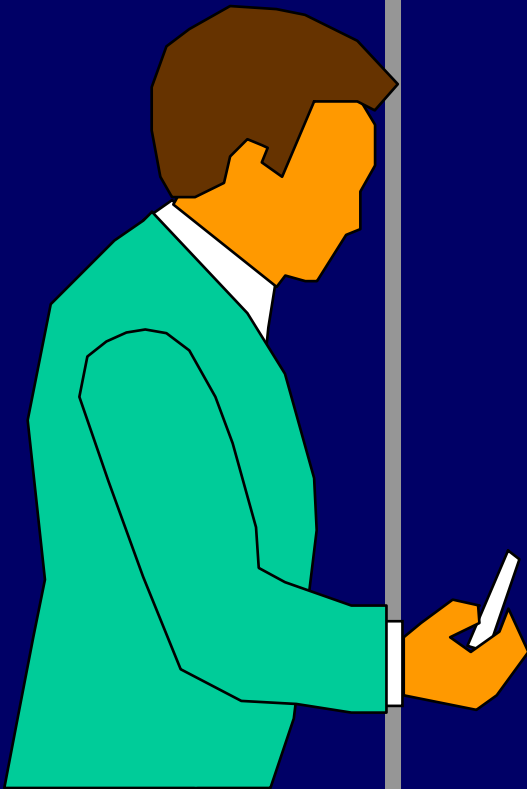


John Bartlett
NetForecast, Inc.
john@netforecast.com
www.netforecast.com

Agenda



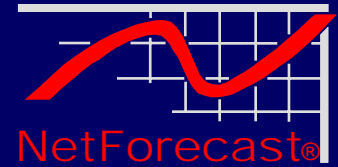
- **Signaling – How to connect**
- **Transport – QoS and Bandwidth**
- **Security – Protecting the equipment, the call and the network**
- **Reliability – Pushing the network to five 9s**



- **Signaling – How to connect**
- Transport – QoS and Bandwidth
- Security – Protecting the equipment, the call and the network
- Reliability – Pushing the network to five 9s

- **How to get the endpoints connected to each other**
- **Simplest method:**
 - Connect endpoints by using DNS names or IP addresses
- **More complex approaches allow:**
 - Dialing by name or phone number
 - Integration with ISDN / PSTN
 - Least cost routing
 - LDAP integration
 - Integration with instant messaging and/or phone
 - Scheduled meeting / automatic setup
- **H.323 vs. SIP**

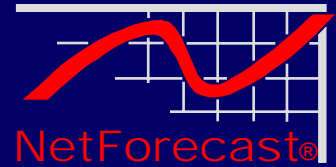
Gatekeeper / Call Manager



- **Centralized server that manages signaling connections**
- **Endpoints register with the GK/CM**
- **Binds names (and E.164 phone numbers) to IP addresses**
- **May integrate with LDAP to authenticate users**

- **Routing signaling through GK/CM adds many features to the multimedia conferencing environment**
 - **PBX-like dialing capabilities**

Instant Messaging Based



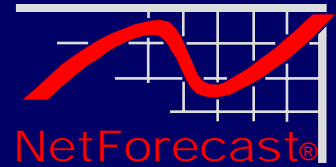
- **Next wave of systems are integrating conferencing with telephony and instant messaging**
- **Concept of being able to ‘upgrade’ a call**
 - **Start with IM**
 - **Upgrade to phone call**
 - **Upgrade to data share**
 - **Upgrade to Video**
 - **Skype does this today! (albeit not business quality)**
- **Most of the ‘feature set’ comes from sophisticated ways of signaling**

Complexity of Multipoint

- Multipoint calls require a 'bridge' to mix or switch the signals
- Bridge resources need to be signaled automatically as a part of call setup
- Bridge resources may need to be scheduled for better utilization
- Bridge can be set up to automatically set up a pre-scheduled call
- Bridge can be used as gateway to ISDN or PSTN connections



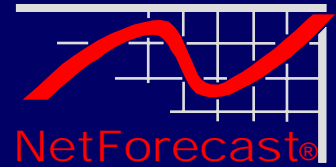
Scheduled Calls vs. Ad Hoc



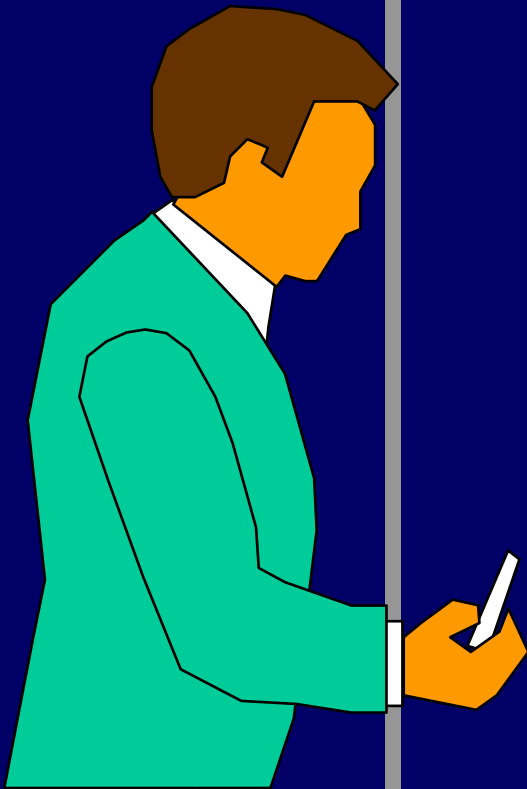
- Heavily managed environments schedule and manage all video calls
- Resource utilization and quality can be kept high
- Easier to manage resources

- Ad hoc calling requires bandwidth and bridge resources to be available
 - Or accept a 'busy signal'
 - Or allow rerouting via the PSTN or alternate IP resources
- Creates lower average utilization because you need to leave 'headroom' for ad hoc calls

Accounting and Utilization

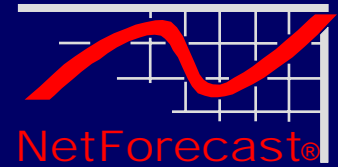


- Gatekeeper and Call Manager allow and track all calls
- Provides information for management such as:
 - Utilization
 - How often are resources being used? How much?
 - Is it time to increase capacity
 - Accounting
 - Allocation of costs to cost centers based on usage

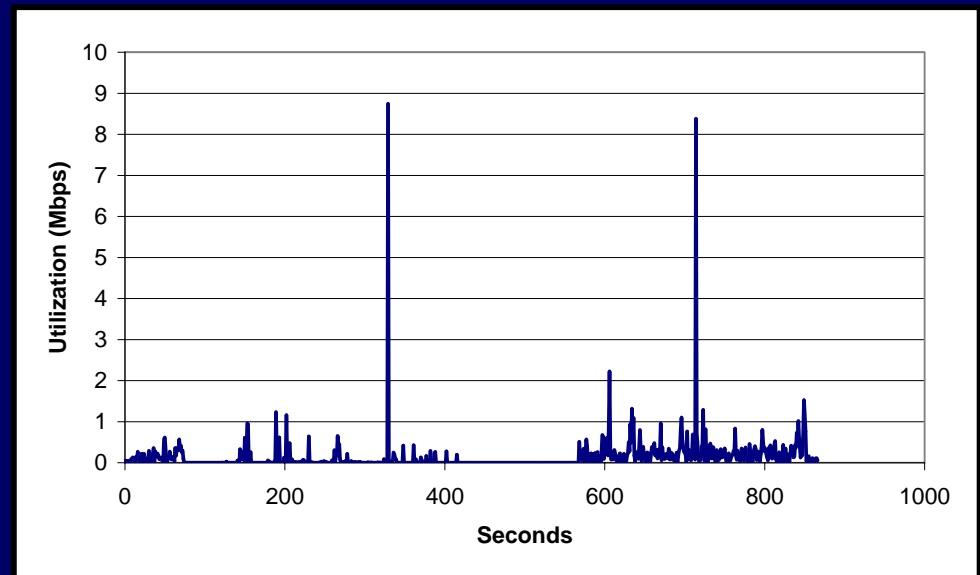


- Signaling – How to connect
- **Transport – QoS and Bandwidth**
- Security – Protecting the equipment, the call and the network
- Reliability – Pushing the network to five 9s

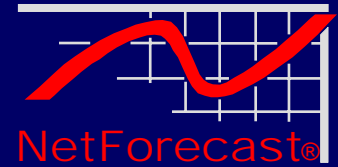
Data Traffic Characteristics



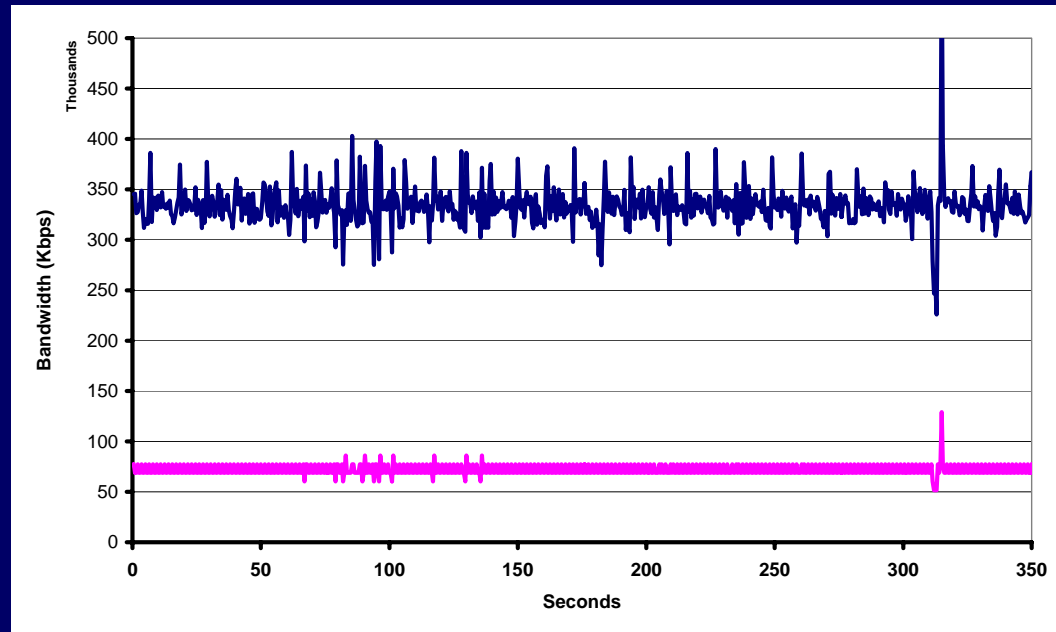
- Data traffic is very bursty, often peaking an order of magnitude above the average traffic level
- Data traffic depends on peak bursts to obtain application performance
- Data traffic easily recovers from packet loss, TCP uses loss to manage bandwidth
- Data traffic degrades gracefully as bandwidth becomes scarce
- Of primary importance – data must arrive 100% correct



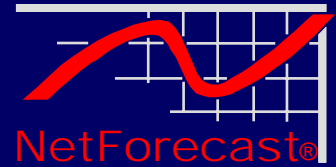
Real-time Traffic Characteristics



- Voice and video encode a continuous stream of data to capture and transfer speech or images
- Bandwidth is capped by the codec algorithm
- Voice / Video quality relies on delivery of all packets
- Voice / Video degrades abruptly when packets are lost
- Of primary importance – packets must be delivered, and delivered in a timely manner



Real-Time Traffic Summary



- **Voice / Video packets must be delivered, and delivered in a timely manner (i.e. low packet loss, low jitter)**
- **There is no time to retransmit a lost packet, so lost packets cause poor quality**
- **Data traffic will interfere with this goal**
- **QoS is required to keep voice & video separated from normal data traffic**

Queues cause Jitter and Loss

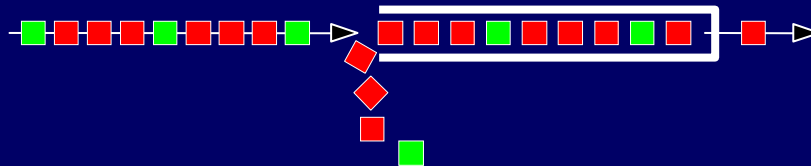
Packets pass through queues in switches and routers



Queue depth affects delay, causing jitter



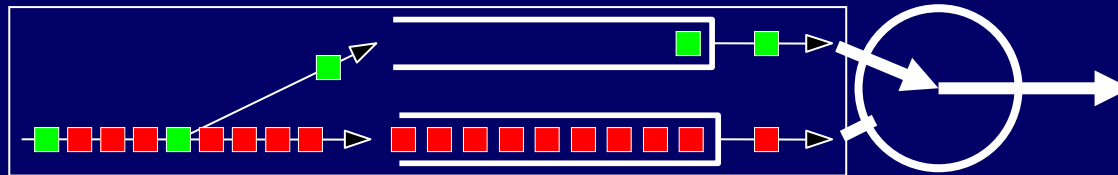
Insufficient bandwidth causes packet loss



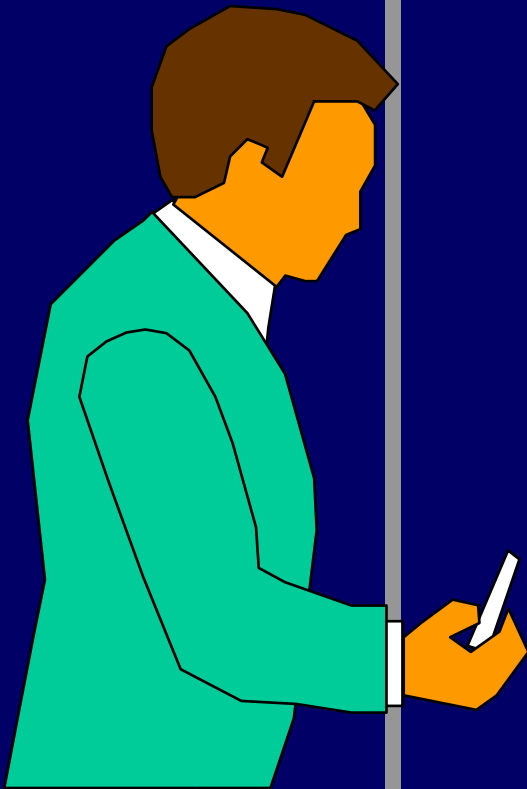
QoS Uses Additional Queues

- An additional high-priority queue is created
- Traffic is identified as being 'high priority'
- High priority traffic is queued in the high priority queue
- The high priority queue is always emptied before lower priority traffic is forwarded

Priority queues allow high priority traffic to bypass slow data queues



Additional queues cause processing loads for the routers



- Signaling – How to connect
- **Transport – QoS and Bandwidth**
- Security – Protecting the equipment, the call and the network

- Reliability – **Classification** network to

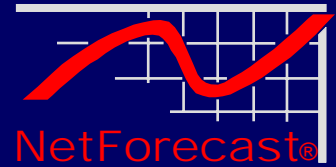
five 9s

Network QoS Implementation

Bandwidth Management

Testing, Measuring and Monitoring

Classification

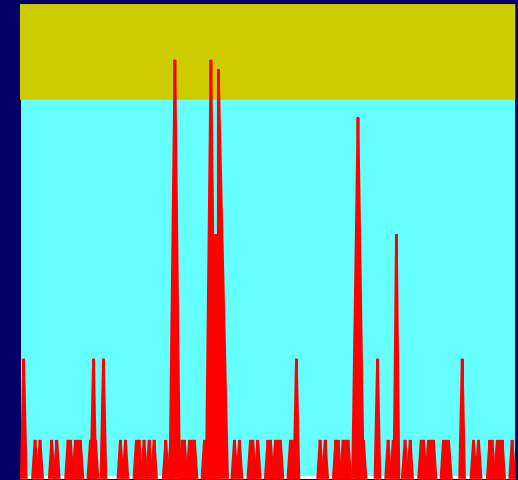
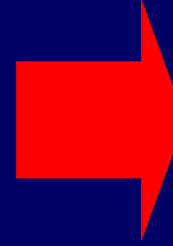
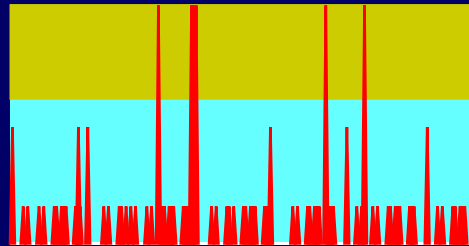


- This is the job of deciding which traffic is high priority traffic, and which is not
- Decision made by endpoint or edge router or a combination of both
- Decision-maker marks packets so core routers can switch packets with appropriate priority
- End point vs. network
 - Multimedia clients/servers can mark their traffic with DiffServ code point to identify it as high priority
 - Endpoint is the best place to distinguish between real-time and other traffic, because it is close to the application
 - Network may not want to trust the endpoint to determine priority
 - Has a more global point of view
 - Distrust of end user (gamer? hacker?)
 - Network has to manage total amount of high priority traffic
 - Who gets to decide?

1. Classification
2. QoS Implementation
3. Bandwidth Mgmt
4. Testing

Over Provision (add Bandwidth)

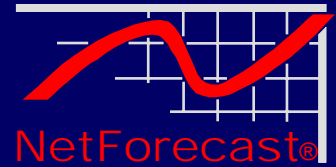
- Adding bandwidth allows real-time traffic and data traffic to coexist



- Inexpensive in the LAN, expensive in the WAN
- Works some of the time ...
- Over provisioning is a statistical game, loss still occurs
- TCP applications expand to take advantage of available bandwidth
- Traffic growth will shift the balance again, causing packet loss
- Requires constant monitoring of utilization and loss to insure success

1. Classification
2. **QoS Implementation**
3. Bandwidth Mgmt
4. Testing

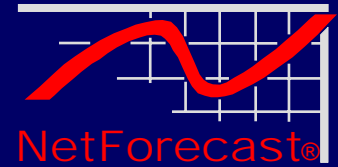
Level 2 QoS, IEEE 802.1p



- **Switches provide priority through IEEE 802.1p**
 - Packets carry a special header behind the Ethernet header
 - Three bits specify a priority level between 0 and 7
- **802.1p priority is often coupled with VLANs (IEEE 802.1Q)**
- **Many enterprise implementations use VLANs to**
 - Isolate video and voice equipment from the data traffic
 - Identify the traffic as voice or video
 - Give priority to traffic on that VLAN
- **QoS is important even on big LAN links where it appears there is plenty of bandwidth!**

1. Classification
2. **QoS Implementation**
3. Bandwidth Mgmt
4. Testing

Level 3 QoS, DiffServ

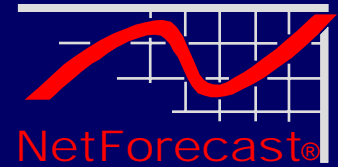


- DiffServ is the standard for Level 3 QoS
- WAN service providers almost all use DiffServ
- DiffServ does not guarantee sufficient bandwidth is available

- Endpoints can mark packets with DiffServ code point
- Edge routers can police or modify those markings to insure consistency
- Core routers treat each class of traffic with appropriate priority
- Requires bandwidth management to insure traffic classes are not over-utilized

1. Classification
2. **QoS Implementation**
3. Bandwidth Mgmt
4. Testing

WAN QoS Implementation



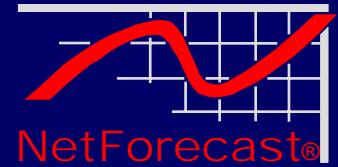
- **If the WAN is direct links owned or leased by the enterprise:**
 - WAN can be treated the same way as LAN (see above) except,
 - Over provisioning is not usually an economically viable alternative

- **If the WAN is a service provider:**
 - Frame Relay, MPLS or VPN
 - May not offer QoS
 - QoS offered is usually DiffServ based

- **Service provider may not implement QoS in the core**
 - But will carry DiffServ markings through their cloud
 - Make sure they will prioritize traffic onto the access link

1. Classification
2. **QoS Implementation**
3. Bandwidth Mgmt
4. Testing

Bandwidth Management

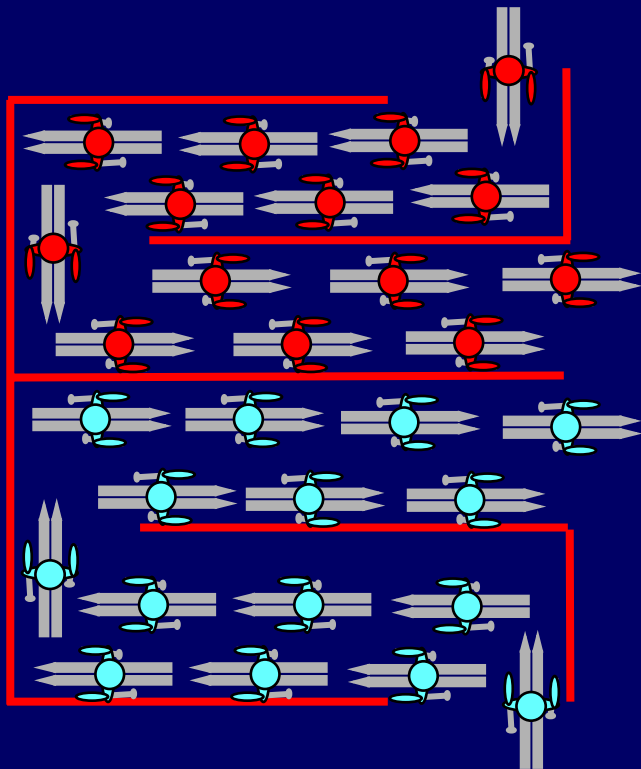


- Quality of Service only works on a limited percentage of the link bandwidth
- When all the traffic is high priority traffic, there is no QoS
- We have to manage the amount of high priority traffic in our networks to insure QoS will work as planned

1. Classification
2. QoS Implementation
3. **Bandwidth Mgmt**
4. Testing

Bandwidth Management

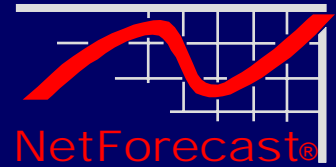
- Priority mechanisms only work if the prioritized traffic is a low percentage of overall traffic



Too many patrol skiers cause queuing, delay, jitter

Low priority (paying) skiers are choked out by high priority excess

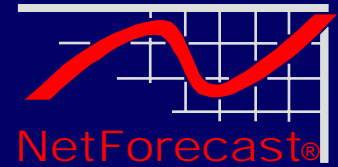
Network Testing, Required!



- We have to test the network and monitor the call quality to know what is going on
 - Are we delivering the quality voice/video service we want to?
 - Is the problem with the voice equipment, or the transport?
 - Where and when is the network causing problems?
- Must test as close to end-to-end as possible
 - Voice is subject to very local problems (echo, local connection, poor equipment) as well as network problems
- Must isolate problems in the network
 - So this call had poor quality, which part of this complex network caused the problem?
- Must find problems in time domain
 - Micro-outages cause momentary burst packet loss
 - Testing or sniffing after the fact has little value

1. Classification
2. QoS Implementation
3. Bandwidth Mgmt
4. **Testing**

Testing Vendors and Tools



● Qualify the Network

- Ixia Chariot
- NetIQ Vivinet Assessor
- Viola NetAssessor

● Monitor the network

- Acterna PVA-1000
- Brix
- NetIQ Vivinet Manager
- Qovia
- RADcom Performer
- Telchemy Vqmon
- Viola NetAssessor
- Prominence

● Debug the Network

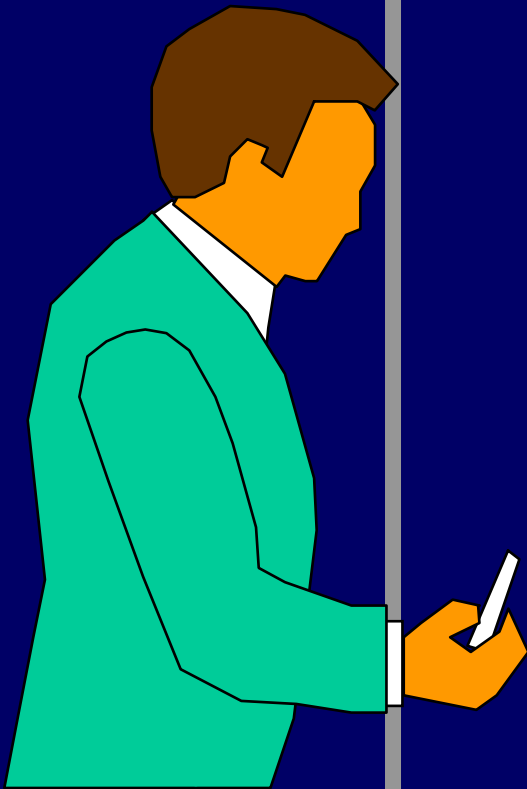
- Acterna PVA-1000
- Ixia Chariot
- NetIQ Vivinet Diagnostics

● Consider stats in the endpoints

● Collect and database Call Data Records (CDRs)

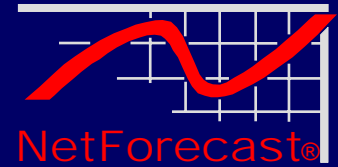
1. Classification
2. QoS Implementation
3. Bandwidth Mgmt
4. **Testing**

Agenda



- Signaling – How to connect
- Transport – QoS and Bandwidth
- **Security – Protecting the equipment, the call and the network**
- Reliability – Pushing the network to five 9s

Video Conferencing Security



- **Securing the Video Conferencing Infrastructure**
 - **Video Conferencing Endpoints**
 - **Video Conferencing Infrastructure**
 - Gatekeeper, Gateway, Bridge, Management
 - **Network components**
 - Routers, switches and firewalls
- **Securing the Video Conference**
 - **Authentication** – Identifying endpoints and users
 - **Authorization** – Determining who is allowed to call whom
 - **Confidentiality** – Insuring the conference is secure
 - **Non Repudiation** – Ability to record the conference
 - **Integrity** – Insuring conference is delivered as sent
- **Allowing Calls Across the Firewall**

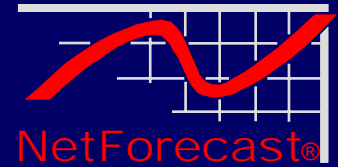
Video Endpoint and Infrastructure Security

Goal: Limit access to endpoints and infrastructure components to those people who are authorized to configure and provision the endpoints

- **VLANs can be used to isolate video conferencing endpoints from other traffic flows**
- **If endpoints do not mark VLAN flows, then administrative traffic must use the same VLAN**
- **Admin access to the VLAN can be limited by a router ACL**
- **VLAN strategy is compatible with Level 2 QoS recommendation (IEEE 802.1p/Q)**

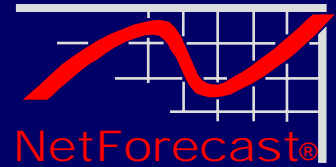


Video and Audio Stream Security



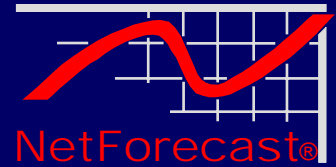
- **Security of video and audio content is insured by encrypting content between endpoints (or endpoint and bridge, or endpoint and gateway)**
- **AES Encryption (per ITU Standard H.235) encrypts the contents of the audio, video and data sharing content streams**
- **Encrypting at endpoint allows QoS markings to be carried through network, no impact on QoS**
- **More sophisticated encryption requires external encryptors at the interface to the WAN**

Passing Thru Firewalls



- **Firewalls are designed to open ports initiated inside the firewall, and allow flows for the duration of a session**
- **H.323 and SIP Require Many Flows**
 - Setup and control flow
 - Video content $A \Rightarrow B$, and $A \Leftarrow B$
 - Audio content $A \Rightarrow B$, and $A \Leftarrow B$
 - Data sharing content $A \Rightarrow B$, and $A \Leftarrow B$
 - RTCP connection for quality information
- **Port assignments are dynamic, information is buried at the application level**

Three Problems to Solve



● Firewall must be application aware

- Find the dynamically assigned UDP port numbers for audio and video streams, open and close at the right times
- Find embedded IP addresses in signaling protocol, translate at the NAT boundary (same problem as FTP)

● Gatekeeper access

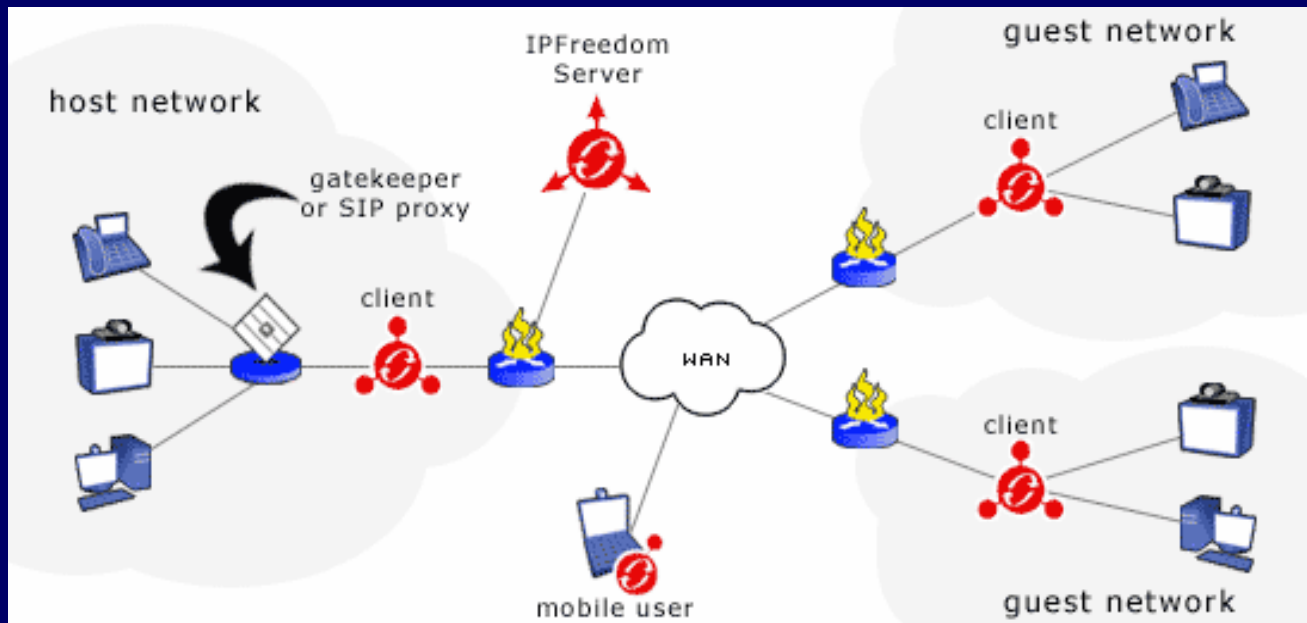
- Calls originating inside and outside the firewall must both have access to a gatekeeper to 'find' the other endpoint
- External gatekeeper has to be protected (not hacked)
- Gatekeepers must peer to exchange endpoint information

● Security

- Need to insure hackers can not cross firewall through temporarily open ports. Application Level Gateways insure only voice and video cross the firewall boundary

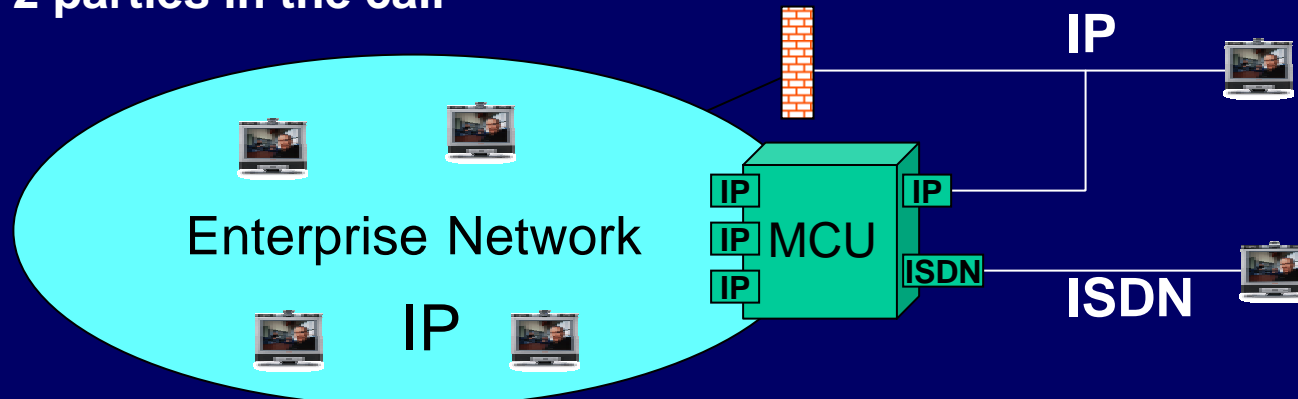
Tandberg Express

- Implementation of GK/Proxy outside firewall
- Express provides external rendezvous point
- All clients calling outside network tunnel through firewall to Express server (IP Freedom Server)



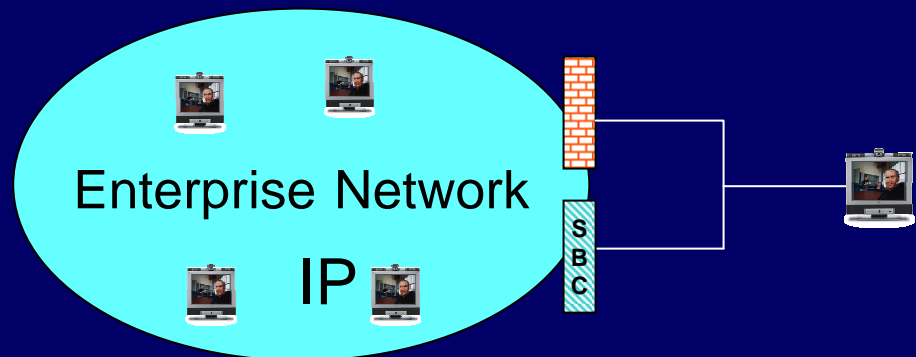
Application Layer Gateway / SBC

- An Application Layer Gateway (ALG) terminates and recreates packet streams at the application layer
- Makes it difficult for hackers to spoof the connection
- MCU can be used as an ALG
 - Attach bridge IP port to either side of a firewall
 - All calls need to 'conference' on the bridge, even if there are only 2 parties in the call

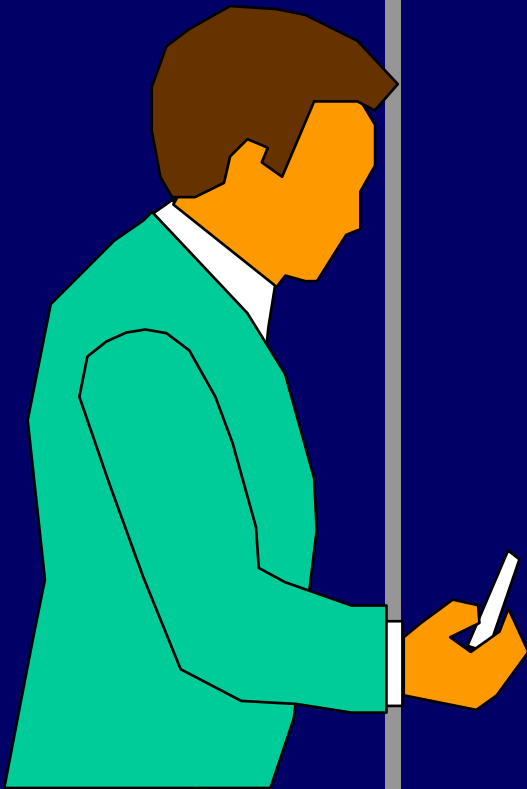


Session Border Controller

- SBC acts as Application Gateway & Gatekeeper
- SBC translates addresses
- SBC may offer QoS and traffic shaping
- Works in parallel with standard firewall
 - Or can be used as stand-alone firewall for data and video
- Scales well by adding capacity as needed per geographic site
- Eliminates hair-pinning

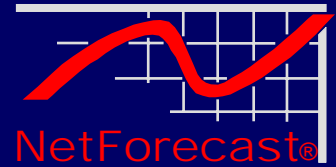


Agenda



- Signaling – How to connect
- Transport – QoS and Bandwidth
- Security – Protecting the equipment, the call and the network
- **Reliability – Pushing the network to five 9s**

What is our Goal?

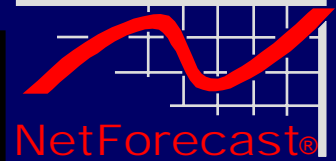


- **We are trying to prevent service failures**
 - Network failures may cause service failures (single point of failure)
 - In redundant networks, a network failure may not cause a service failure because of redundant components
 - Service failures can occur without a network failure due to momentary problems like congestion or reconfiguration

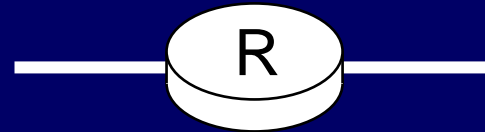
- **Keep the overall goal in mind during design and testing phases**

Let's Do The Math

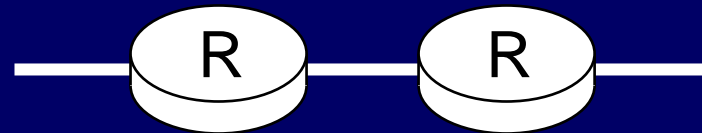
Assume:
Reliability of Router
is 90% (0.9)



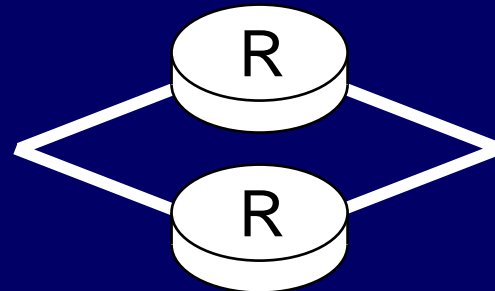
Reliability of this
network = 90%



Reliability of two
routers in series =
 $0.9 \times 0.9 = 81\%$

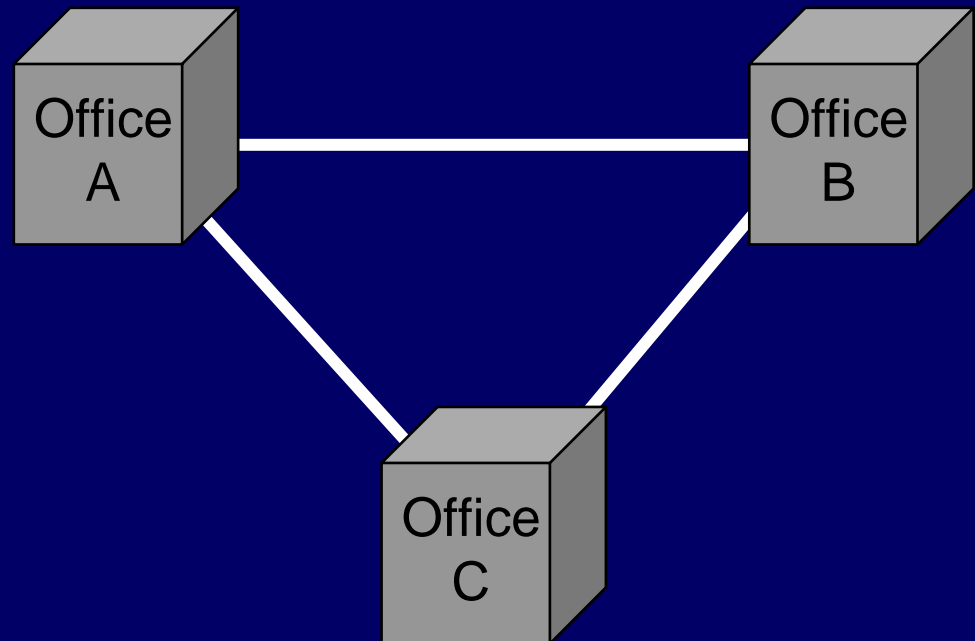


Reliability of two
routers in parallel =
 $(1-0.9) \times (1-0.9) = 1-R$
 $R = 99\%$



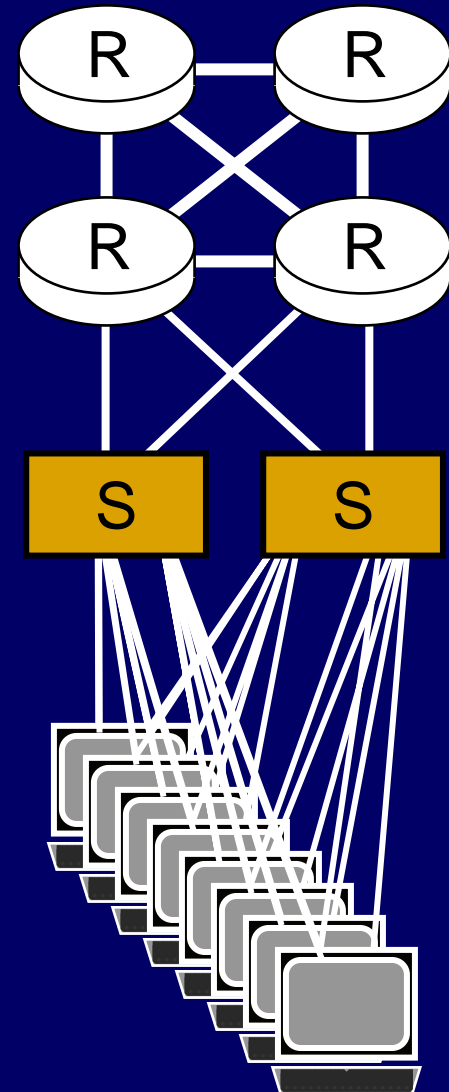
WAN Redundancy

- **Multiple connected offices provide redundant connections**
- **May be lower cost solution than parallel links**
- **Larger configurations have tradeoffs**
 - **Full mesh connectivity**
 - **Fewer connections, but longer distances between sites, especially when failures occur**

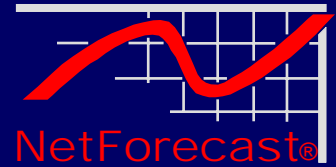


LAN Redundancy

- Core is connected as mesh
- Switches redundantly connected to core
- Endpoint Options
 - Singly connected
 - Interleaved
 - Redundantly connected
- How important is each terminal?
- How many users are affected by each failure?

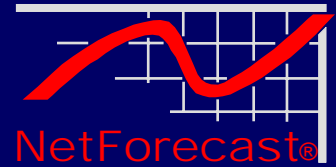


How Much Resilience Do I Need?



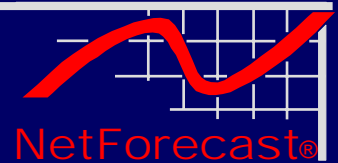
- **Big tradeoff between cost and return**
- **Do the risk analysis**
 - **Collect facts and assumptions on network outages**
 - **Understand number of employees or customers affected**
 - **Estimate probability and financial impact of outages**
- **Understand assumptions about event independence**
 - **Malicious attacks may break event independence model**
 - **Large events (storm, quake, power failure) may break event independence model**

References



- **“Data Networks, Routing Security and Performance Optimization”, Tony Kenyon, ISBN 1-55558-271-0**
- **“Issues on Resilient Design, The Cat’s Cradle Effect”, White Paper by John Herbert, INS**

Thank you! Questions?



Some reference information:

“Economics of QoS on WAN Access Lines”, Business Communications Review, October 2004 issue, p16 by Bartlett, Moore and Sevcik

“Understanding Web Performance”, Business Communications Review, October 2001, p28 by Sevcik and Bartlett

NetForecast Report 5075 “Real Time Applications on IP Networks: Overcoming Economic Constraints on Quality of Service”

“Data Networks, Routing Security and Performance Optimization”, Tony Kenyon, ISBN 1-55558-271-0

“Issues on Resilient Design, The Cat’s Cradle Effect”, White Paper by John Herbert, INS

- Reports and articles available at www.netforecast.com

John Bartlett can be reached at: john@netforecast.com